(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年10 月14 日 (14.10.2004)

PCT

(10) 国際公開番号
WO 2004/088557 A1

(51) 国際特許分類[7]: G06F 17/60

(21) 国際出願番号: PCT/JP2004/004338

(22) 国際出願日: 2004 年3 月26 日 (26.03.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-092647 2003 年3 月28 日 (28.03.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 板橋 達夫 (ITABASHI, Tatsuo) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

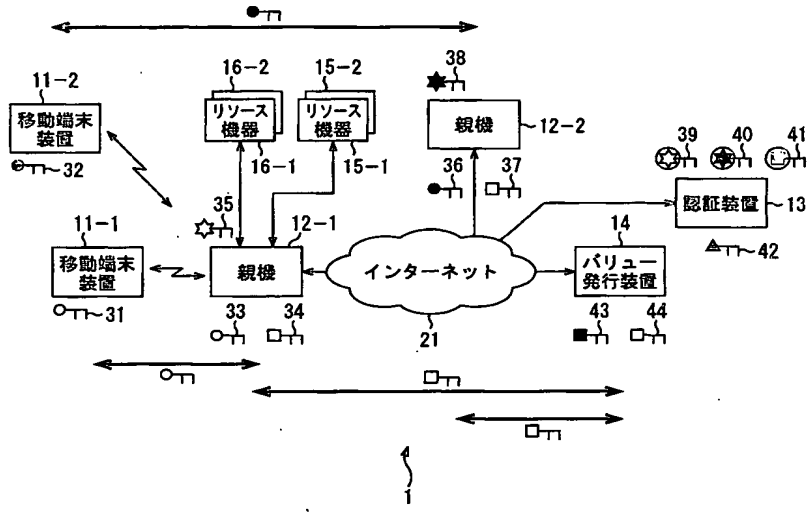
(74) 代理人: 稲本 義雄 (INAMOTO, Yoshio); 〒1600023 東京都新宿区西新宿７丁目１１番１８号 ７１１ビルディング４階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[続葉有]

(54) Title: INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING DEVICE, METHOD, AND PROGRAM

(54) 発明の名称: 情報処理システム、情報処理装置および方法、並びにプログラム



11-2... MOBILE TERMINAL DEVICE
16-2... RESOURCE DEVICE
15-2... RESOURCE DEVICE
12-2... PARENT DEVICE
11-1... MOBILE TERMINAL DEVICE
12-1... PARENT DEVICE
21... INTERNET
14... VALUE ISSUING DEVICE
13... AUTHENTICATION DEVICE

(57) Abstract: An information processing system, an information processing device, method, and program for a moving user to operate a device in a moved space anonymously. A mobile terminal device (11-2) requests a parent device (12-2) for a resource of a resource device (15). The parent device (12-2) requests a parent device (12-1) for resource permission and the parent device (12-1) notifies consideration required for permitting the resource to the parent device (12-2). The parent device (12-2) requests a value issuing device (14) to transfer the consideration. The value issuing device (14) transfers the consideration of the parent device (12-2) to the parent device (12-1) and transmits a transfer notification to the parent device (12-1). The parent device (12-1) receives the transfer notification and gives the right to use the resource via the parent device (12-2) to the mobile terminal device (11-2). The present invention can be applied to a radio communication system.

[続葉有]

WO 2004/088557 A1

SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 本発明は、ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作することができるようにする情報処理システム、情報処理装置および方法、並びにプログラムに関する。移動端末装置１１−２は、親機１２−２にリソース機器１５のリソースを要求する。親機１２−２は、親機１２−１にリソース許可を要求し、親機１２−１は、親機１２−２に対してリソースを許可するために必要な対価を通知する。親機１２−２は、バリュー発行装置１４に対価の移動を要求する。バリュー発行装置１４は、親機１２−２の対価を親機１２−１に移動し、振込み通知書を親機１２−１に送信する。親機１２−１は、その振込み通知書を受信し、リソース利用の権利を親機１２−２を経由して移動端末装置１２−２に与える。本発明は、無線通信システムに適用することができる。

明細書

情報処理システム、情報処理装置および方法、並びにプログラム

技術分野

本発明は、情報処理システム、情報処理装置および方法、並びにプログラムに関し、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のままユーザの嗜好に合わせた操作性で操作させることができるようにした情報処理システム、情報処理装置および方法、並びにプログラムに関する。

背景技術

近年、携帯型のパーソナルコンピュータ、携帯電話などが普及し、多くのユーザがこれら通信機能、情報処理機能を有する小型の装置を携帯し、屋外で、あるいは移動先においてネットワークに接続してネットワークを介する通信を行なっている。

ここで、既存のインフラを利用したシステムとして、すでに存在する様々な通信網を適宜切り替えて利用するパーソナル通信サービス分散システムが提案されている（例えば、特開平８－５６２６３号公報）。このシステムは、例えば電子メールサービスや電話サービス等の異なるネットワーク通信網を統合して利用することを可能としたシステムである。

しかしながら、このようなシステムにおいて、ユーザが外出中のような状況で、ユーザにメッセージを伝達することはできても、出先に有るたまたま身近な機器を、自らの所有する同種機種と同じ感覚で利用するなど、周囲に置いてある機器を自分に合わせた使い方をすることはできず、結局ユーザは、使い慣れた端末（例えば、ＰＣなど）を持ち運ばなくてはならなかった。

このような問題に対して、自宅のホームサーバに自分の嗜好等の情報を持ち、その情報を基に出先の機器の振る舞いを変化させるシステムを、本出願人が先に、特願２００３－２９２５８７号で提案している。

しかしながら、この方法では、一方的に他者のリソースを使い続けるユーザや、他者のリソースを使う機会が少ないにもかかわらず、自ら所有するリソースを提供し続けるユーザがいる場合、需給のバランスがとれなくなる恐れがある。

そこで、ユーザが、他者の所有するリソースを利用するために必要な対価を、自分と他者の対価を管理する装置を介して支払うシステムが必要となる。

このためには、例えばクレジットカード番号をやり取りすることによりリソースの提供者とリソースのユーザ側との間で対価をやり取りする方法が考えられる。

しかしながら、クレジットカード番号はプライバシー情報のため、他者に知られるには抵抗があり、また、クレジットカードを利用するためには自分の個人情報をカード会社に登録しなければならず、つまりユーザの個人情報は対価を管理する装置に管理される。従って、ユーザが対価を管理する装置に対しても匿名のまま対価を支払い、他者の所有するリソースを利用することは困難であった。

このため、対価を前提に公共の場で通信サービスを行っている無線LAN（Local Area Network）等の事業者とのシームレスなサービスをユーザに提供することは困難であった。

発明の開示

本発明は、このような状況に鑑みてなされたものであり、ユーザが移動する場合においても、移動した空間にある機器を、自分の慣れ親しんだ操作方法で操作できるなど、自分の嗜好などの個人の情報を基に機器の動作を変化させ、かつ匿名のままその対価を支払うことができるようにするものである。

本発明の情報処理システムは、ユーザにより操作される端末と、リソースを提供する第１の親機と、ユーザの個人情報を記憶する第２の親機と、電子バリューを管理するバリュー装置とを備える情報処理システムであって、端末は、第１の親機が提供するリソースを要求する信号を、第２の親機に送信するリソース要求信号送信手段と、第１の親機が提供するリソースを利用する利用権を、第２の親機から取得する第１の利用権取得手段とを有し、利用権を、第１の親機に提示し

て、第１の親機が提供するリソースを利用し、第１の親機は、リソースの提供に対する対価としての電子バリューが、第２の親機から第１の親機に振り込まれたことの振込み通知を、バリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、第２の親機に対して、利用権を発行する利用権発行手段とを有し、端末が、利用権を提示した場合に、自身が有するリソースの利用を許可し、第２の親機は、端末装置から送信されてくる、リソースを要求する信号に応じて、第１の親機への電子バリューの振込みを、バリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、第１の親機が発行する利用権を取得する第２の利用権取得手段と、第２の利用権取得手段において取得された利用権を、端末に提供する利用権提供手段とを有し、バリュー装置は、第２の親機からの要求に応じて、第１の親機に電子バリューを振り込む電子バリュー振込み手段と、第１の親機への電子バリューの振込み通知を、第１の親機に送信する振込み通知送信手段とを有することを特徴とする。

本発明の第１の情報処理装置は、リソースを提供する第１の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信手段と、第１の親機が提供するリソースを利用する利用権を、第２の親機から取得する利用権取得手段とを備え、利用権を、第１の親機に提示して、第１の親機が提供するリソースを利用することを特徴とする。

第２の親機との間で、ユーザが第２の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

リソース要求信号送信手段と利用権取得手段は、第１の親機を介して、第２の親機とやりとりするようにすることができる。

リソース要求信号送信手段と利用権取得手段は、第２の親機との間で、データを暗号化してやりとりするようにすることができる。

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

本発明の第１の情報処理装置の情報処理方法は、リソースを提供する第１の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信ステップと、第１の親機が提供するリソースを利用する利用権を、第２の親機から取得する利用権取得ステップとを含み、利用権を、第１の親機に提示して、第１の親機が提供するリソースを利用することを特徴とする。

本発明の第１の情報処理装置のプログラムは、リソースを提供する第１の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信ステップと、第１の親機が提供するリソースを利用する利用権を、第２の親機から取得する利用権取得ステップとを含み、利用権を、第１の親機に提示して、第１の親機が提供するリソースを利用することを特徴とする。

本発明の第２の情報処理装置は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段とを備え、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

振込み通知が正当であることの認証を行う認証手段をさらに備えるようにすることができる。

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

本発明の第２の情報処理装置の情報処理方法は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通

知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

本発明の第２の情報処理装置のプログラムは、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

本発明の第３の情報処理装置は、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段と、利用権取得手段において取得された利用権を、端末に提供する利用権提供手段とを備えることを特徴とする。

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

端末との間で、ユーザが個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

本発明の第３の情報処理装置の情報処理方法は、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、そ

の親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供ステップとを含むことを特徴とする。

本発明の第３の情報処理装置のプログラムは、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供ステップとを含むことを特徴とする。

本発明の第４の情報処理装置は、ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込み手段と、第２の親機から第１の親機への電子バリューの振込みが行われたことを表す振込み通知を、第１の親機に送信する振込み通知送信手段とを備えることを特徴とする。

第１または第２の親機との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

第１と第２の親機の電子バリューを記憶する記憶手段をさらに備え、電子バリュー振込み手段は、記憶手段に記憶された電子バリューを書き換えることにより、第２の親機から第１の親機に対して、電子バリューを振り込むようにすることができる。

電子バリュー振込み手段は、第２の親機から電子バリューを取得し、その電子バリューを第１の親機に送信することにより、第２の親機から第１の親機に対して、電子バリューを振り込むようにすることができる。

本発明の第４の情報処理装置の情報処理方法は、ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価と

しての電子バリューの振込みを、ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込みステップと、第２の親機から第１の親機への電子バリューの振込みが行われたことを表す振込み通知を、第１の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

本発明の第４の情報処理装置のプログラムは、ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込みステップと、第２の親機から第１の親機への電子バリューの振込みが行われたことを表す振込み通知を、第１の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

本発明においては、端末により、第１の親機が提供するリソースを要求する信号が、第２の親機に送信され、記第１の親機が提供するリソースを利用する利用権が、第２の親機から取得される。そして、利用権が、第１の親機に提示され、第１の親機が提供するリソースが利用される。また、第１の親機により、リソースの提供に対する対価としての電子バリューが、第２の親機から第１の親機に振り込まれたことの振込み通知が、バリュー装置から受信され、振込み通知に応じて、第２の親機に対して、利用権が発行される。また、第１の親機により、端末により利用権が提示された場合に、自身が有するリソースの利用が許可される。第２の親機により、端末装置から送信されてくる、リソースを要求する信号に応じて、第１の親機への電子バリューの振込みが、バリュー装置に要求され、電子バリューの振込みに応じて、第１の親機が発行する利用権が取得される。また、第２の親機により、取得された利用権が、端末に提供される。バリュー装置により、第２の親機からの要求に応じて、第１の親機に電子バリューが振り込まれ、第１の親機への電子バリューの振込み通知が、第１の親機に送信される。

図面の簡単な説明

図１は、本発明を適用した通信システムの構成例を示すブロック図である。

図２は、図１の移動端末装置の構成例を示すブロック図である。

図３は、図２の移動端末装置におけるリソース取得処理を説明するフローチャートである。

図４は、図３のステップＳ２およびステップＳ６の共通秘密鍵認証処理を説明するフローチャートである。

図５は、図３のステップＳ５のリソース情報取得処理を説明するフローチャートである。

図６は、図１の親機の構成例を示す図である。

図７は、図６のリソース制御部の構成例を示す図である。

図８は、図６の親機におけるリソース制御処理を説明するフローチャートである。

図９は、図８のステップＳ７１のリソース送信処理を説明するフローチャートである。

図１０は、図８のステップＳ７１のリソース送信処理を説明するフローチャートである。

図１１は、電子証明書の例を示す図である。

図１２は、図６の親機におけるリソース情報送信処理を説明する図である。

図１３は、図６の親機におけるリソース利用条件文発行処理を説明するフローチャートである。

図１４は、図６の親機における権利文発行要求処理を説明するフローチャートである。

図１５は、図１のバリュー発行装置の構成例を示す図である。

図１６は、図１５のバリュー発行装置における振込み通知書送信処理を説明するフローチャートである。

図１７は、図１の認証装置の構成例を示す図である。

図１８は、図１７の認証装置における電子証明書判定処理を説明する図である。

図１９は、図１の通信システムにおけるリソース取得処理を説明する図である。

図２０は、他のシステムの構成例を示す図である。

図２１は、図２０に示したシステムの動作を説明するフローチャートである。

発明を実施するための最良の形態

以下、図を参照し本発明の実施の形態について説明する。

図１は、本発明を適用した情報処理システム１の構成例を示すブロック図である。

この情報処理システム１では、親機１２とバリュー発行装置１４間の処理を安全確実に行うために用いられた公開鍵暗号（PKI（Public Key Infrastructure））系の暗号技術を用いてセキュリティを確保する。

図１の例においては、２人のユーザが、それぞれ移動端末装置１１－１と移動端末装置１１－２を有している。ユーザは、必ず１つの親機にユーザの個人情報（利用履歴、嗜好、決済関連等）を格納し、ユーザの認証情報として共通秘密鍵を取得する。この例では、ユーザと親機が共通秘密鍵として同じパスフレーズを有しており、ユーザと親機は、同じパスフレーズを有することを確認することで、ユーザを認証する。

また、この例では、移動端末装置１１－１のユーザは親機１２－１に、移動端末装置１１－２のユーザは親機１２－２に、ユーザの個人情報を格納している。

さらに、移動端末装置１１－１は、その移動端末装置１１－１のユーザの個人情報を格納した親機１２－１と直接無線で通信可能な位置にあり、移動端末装置１１－２は、その移動端末装置１１－２のユーザの個人情報を格納した親機１２－２とは遠隔地に設置された、親機１２－１と直接無線で通信できる位置にある。従って、移動端末装置１１－２は、親機１２－２とは無線で通信することが困難であるが、親機１２－１とは直接無線で通信できる。

移動端末装置１１－１と移動端末装置１１－２は、ユーザとともに移動し、無線通信を用いてユーザからの指示に対応する信号を親機１２－１に送信する。また、移動端末装置１１－１と移動端末装置１１－２は、無線通信を用いて、親機１２－１からの信号を受信する。

以下、移動端末装置１１－１と移動端末装置１１－２のそれぞれを個々に区別する必要がない場合、適宜、まとめて、移動端末装置１１と称する。

この移動端末装置１１とユーザとは、依存関係がなく、ユーザが移動端末装置１１を利用するときにのみ、移動端末装置１１は、ユーザの認証を行う。従って、移動端末装置１１には、ユーザの認証情報の入力機能が備えられている。

図１の例においては、移動端末装置１１－１および移動端末装置１１－２のユーザは、ユーザの認証情報として、共通秘密鍵３１および共通秘密鍵３２を、それぞれ入力している。

親機１２－１は、所定の空間に配置され、無線通信を用いて、移動端末装置１１から送信された信号を受信するとともに、移動端末装置１１に信号を送信する。また、親機１２－１は、ユーザに提供する情報であるコンテンツ等のリソースを有するリソース機器１５－１、リソース機器１５－２、リソース機器１６－１、およびリソース機器１６－２と接続されている。さらに、親機１２－１は、インターネット２１を介して、認証装置１３およびバリュー発行装置１４と接続されている。

ここで、親機１２－１は、例えば、移動端末装置１１－１のユーザのユーザ宅の、いわゆるホームサーバで構成することができる。同様に、親機１２－２も、例えば、移動端末装置１１－２のユーザのユーザ宅のホームサーバで構成することができる。

以下、リソース機器１５－１とリソース機器１５－２のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器１５と称する。また、リソース機器１６－１とリソース機器１６－２のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器１６と称する。

これにより、移動端末装置１１は、親機１２－１を介して、親機１２－１に接続されたリソース機器１５、リソース機器１６、およびインターネット２１を介して接続された機器との通信ができる。

また、親機１２－１は、ユーザの認証情報として共通秘密鍵３３を格納している。即ち、この共通秘密鍵３３は、移動端末装置１１－１のユーザに入力された共通秘密鍵３１と等しくなっている。さらに、親機１２－１は、バリュー発行装置１４により送信された共通秘密鍵３４と、自らの正当性を証明する秘密鍵３５を記憶している。

親機１２－２は、インターネット２１を介して、親機１２－１、認証装置１３、およびバリュー発行装置１４と接続されている。

また、親機１２－２は、ユーザの認証情報として共通秘密鍵３６を格納している。この共通秘密鍵３６は、移動端末装置１１－２のユーザに入力された共通秘密鍵３２と等しくなっている。さらに、親機１２－１は、バリュー発行装置１４により送信された共通秘密鍵３７と、自らの正当性を証明する秘密鍵３８を記憶している。

以下、親機１２－１と親機１２－２のそれぞれを個々に区別する必要がない場合、適宜、まとめて、親機１２と称する。

認証装置１３は、親機１２－１の秘密鍵３５に対応する公開鍵３９、親機１２－２の秘密鍵３８に対応する公開鍵４０、およびバリュー発行装置１４の後述する秘密鍵４３に対応する公開鍵４１を記憶する。また、認証装置１３は、自らの正当性を証明する秘密鍵４２を記憶する。

認証装置１３は、他の装置からの要求に応じて公開鍵を検索し、その公開鍵を他の装置に送信する。秘密鍵とそれに対応する公開鍵は、一方の鍵に基づいて生成された暗号文を他方の鍵を用いて復号できる関係にある。また、認証装置１３は、電子証明書（図１１）の発行および鍵の失効管理を行う。

バリュー発行装置１４は、親機１２－１と親機１２－２に対し、バリュー（電子バリュー）の発行および流通管理を行う。バリュー発行装置１４は、自らの正

当性を証明する秘密鍵４３および共通秘密鍵４４を記憶している。バリュー発行装置１４は、共通秘密鍵４４をバリューを発行する相手である親機１２－１と親機１２－２に送信し、親機１２－１に共通秘密鍵３４として記憶させるとともに、親機１２－２に共通秘密鍵３７として記憶させる。即ち、共通秘密鍵３４、共通秘密鍵３７、および共通秘密鍵４４は等しい。

ユーザは、自身の個人情報（利用履歴、嗜好、決済関連情報等）を自身の親機１２－１，１２－２にのみ格納し、共通秘密鍵３３，３６を取得する。そして、この共通秘密鍵を用いて、全ての通信を行うことにより、ユーザは、匿名性を保ち、安全に通信を行うことができる。

なお、上述の例では、２個の移動端末装置が存在するが、移動中のユーザが多数いる場合、その数だけの移動端末装置が存在するものとする。また、上述の例では、２個の親機が存在するが、各空間には、それぞれの空間に必要な数だけの親機が存在するものとする。

また、共通秘密鍵３１と共通秘密鍵３２は、移動端末装置１１のユーザを認証するための鍵である。共通秘密鍵３４、共通秘密鍵３７、および共通秘密鍵４４は、バリューを扱う正当な装置であることを認証するための鍵である。秘密鍵３５、秘密鍵３８、および秘密鍵４３は、自らの正当性を証明するための鍵であり、装置間における通信中の改ざんを防止する。

以上のように構成される通信システム１によって、例えば、移動端末装置１１－２のユーザがその個人情報を記憶していない親機１２－１のリソースを利用する場合には、移動端末装置１１－２は、親機１２－１の利用したいリソースを指定し、個人情報を記憶している親機１２－２に、そのリソースの利用を要求する。親機１２－２は、移動端末装置１１－２からリソースが要求されると、親機１２－１に対するリソース利用に必要なバリューの支払いを、バリュー発行装置１４に要求する。

バリュー発行装置１４は、親機１２－２のバリューを親機１２－１に移動させ、親機１２－１にバリューの振込みが行われたことを表す振込み通知を発行する。

親機１２－１は、バリュー発行装置１４から振り込み通知を受信すると、親機１２－２にリソースを利用する利用権を発行する。親機１２－２は、親機１２－１から利用権が発行されると、その利用権を移動端末装置１１－２に送信する。移動端末装置１１－２は、その利用権を親機１２－１に提示し、リソースを要求する。親機１２－２は、移動端末装置１１－２から利用権を提示された場合、リソースの利用を許可する。

次に、図２は、図１の移動端末装置１１の詳細構成例を示している。

図２の例では、移動端末装置１１－１を説明するが、移動端末装置１１－２も同様に構成される。

移動端末装置１１－１は、CPU (Central Processing Unit) ６１、ROM(Read Only Memory)６２、RAM(Random Access Memory)６３、表示部６４、リーダライタ６５、送信部６６、アンテナ６７、受信部６８、暗号/復号部６９、および操作入力部７０から構成される。

なお、移動端末装置１１－１のユーザは、あらかじめ取得した共通秘密鍵３１、自身の親機１２－１が接続しているリソースの情報、および自身の親機１２－１のネットワーク上のアドレスを格納した非接触ＩＣ（Integrated Circuit）カード７１を有している。

このように、共通秘密鍵３１を改ざんが困難な非接触ＩＣカードに安全に格納することにより、通信システムの安全性と利便性を向上させることができる。また、非接触ＩＣカードは、非接触のインターフェースであるので、利用時の利便性が向上し、かつ簡単な操作で処理が可能になる。

この非接触ＩＣカードとしては、例えば、FeliCa（商標）のような対タンパ性の高いＩＣチップが用いられる。なお、共通秘密鍵３１などは、非接触型ではなく接触型のデバイスに格納することも可能である。但し、便利性やデバイスの劣化に対する耐性を考えると、接触型ではなく、非接触型を採用するのが望ましい。

CPU６１は、ROM６２に記憶されているプログラムに従って各種の処理を実行する。RAM６３には、CPU６１が各種の処理を実行する上において必要なデータなどが適宜記憶される。

表示部６４は、CPU６１からの指令により、例えば、移動端末装置１１－１が利用できるリソースの情報を表示する。リーダライタ６５は、ユーザが有する非接触ＩＣカード７１に封じ込められた（格納された）共通秘密鍵３１、ユーザの個人情報を記憶した親機１２－１が接続しているリソースの情報、および個人情報を記憶した親機１２－１のネットワーク上のアドレスを読み込み、CPU６１に共通秘密鍵３１、リソース情報、およびアドレスを供給する。ここで、また、リーダライタ６５は、CPU６１からの指令により、必要に応じて非接触ＩＣカード７１にデータを書き込む。

送信部６６は、CPU６１からの指令により、親機１２－１に送信する信号をアンテナ６７に供給する。アンテナ６７は、送信部６６から供給された信号を、無線通信を用いて親機１２－１に送信する。さらに、アンテナ６７は、親機１２－１から送信された信号を受信し、その信号を受信部６８に供給する。受信部６８は、アンテナ６７から供給された信号を、CPU６１に供給する。

暗号/復号部６９は、非接触ＩＣカード７１から読み込まれた共通秘密鍵３１を暗号化したり、受信部６８で受信した暗号化された共通秘密鍵を復号し、その復号した共通秘密鍵をさらに暗号化する。操作入力部７０は、ユーザにより操作され、その操作に対応する信号がCPU６１に供給される。

図３は、図２の移動端末装置１１がリソースを取得する処理を説明するフローチャートである。なお、ユーザは、予め個人情報を自身の親機に格納しており、共通秘密鍵３１（３２）、その親機に接続されているリソースの情報、およびその親機のネットワーク上のアドレスは非接触ＩＣカード７１に記憶されているものとする。図３の処理は、例えば、ユーザが操作入力部７０を操作して親機１２－１に接続されているリソースの取得を要求したときに開始される。

ステップＳ１において、CPU６１は、移動端末装置１１を使用するユーザの個人情報が格納されている自身の親機（以下、適宜、本親機と称する）と無線通信が可能であるかどうかを判定する。例えば、移動端末装置１１は、無線通信が可能な機器を検索し、検索された機器の中に本親機が含まれているかどうかを判定する。

ステップＳ１で、CPU６１は、本親機と無線通信が可能であると判定した場合、ステップＳ２に進み、CPU６１は、本親機（例えば、移動端末装置１１－１の場合、親機１２－１）との間で共通秘密鍵認証処理を行ない、ステップＳ３に進む。この共通秘密鍵認証処理の詳細は、図４で後述する。

ステップＳ３では、CPU６１は、ユーザが操作入力部７０を操作することにより指定したリソースを要求する信号を、送信部６６を制御して、アンテナ６７から本親機である、例えば、親機１２－１に送信する。即ち、ユーザは、非接触ＩＣカード７１に記憶され、リーダライタ６５から読み込まれたリソース情報を表示部６４に表示させ、そのリソース情報を見て、取得したいリソースを指定する。これにより、そのリソースを要求する信号がアンテナ６７から送信される。なお、以下の説明では、CPU６１が送信部６６を制御して、信号を送信することを、単に、CPU６１が信号を送信するという。

ステップＳ３の処理後は、ステップＳ４に進み、アンテナ６７は、ステップＳ３のリソース要求信号に対応して親機１２－１から送信されたリソース（を使用するのに必要な情報）を受信し、受信部６８を介してCPU６１に供給する。そして、CPU６１は、そのリソースをRAM６３に保持する。なお、以下の説明では、アンテナ６７が信号を受信し、受信部６８を介して、CPU６１にその信号を供給することを、単に、CPU６１が信号を受信するという。

一方、ステップＳ１で、CPU６１は、本親機と無線通信が可能ではないと判定した場合（例えば、移動端末装置１１－２が、親機１２－２と通信できない場合）、ステップＳ５に進み、リソース情報取得処理を行ない、ステップＳ６に進む。即ち、例えば、移動端末装置１１－２については、現在、その移動端末装置

１１－２と通信できる親機１２－１が本親機ではないので、移動端末装置１１－２は、親機１２－１が接続しているリソースの情報を非接触ＩＣカード７１に記憶していない。従って、移動端末装置１１－２は、親機１２－１が接続しているリソースの情報を取得する必要があり、このため、ステップＳ５において、リソース情報取得処理が行なわれる。このリソース情報取得処理の詳細は、図５で後述する。

ステップＳ６において、CPU６１は、本親機（親機１２－２）との間で共通秘密鍵認証処理を行い、ステップＳ７に進む。なお、いまの場合、移動端末装置１１－２は、本親機である親機１２－２と直接無線通信することはできないため、ステップＳ６の共通秘密鍵認証処理は、後述するように、移動端末装置１１－２と親機１２－２との間で、親機１２－１およびインターネット２１を介した通信を行うことにより実行される。この共通秘密鍵認証処理の詳細は、図４で後述する。

ステップＳ７では、CPU６１は、非接触ＩＣカード７１から、親機１２－２のアドレスを読み出す。そして、ユーザが操作入力部７０を操作することにより指定したリソースを要求する信号（リソース利用権発行要求）を親機１２－２のアドレスとともに、親機１２－１に送信し、インターネット２１経由で親機１２－２に送信する。即ち、ユーザは、ステップＳ５で取得した親機１２－１が接続しているリソースのリソース情報を表示部６４に表示させ、そのリソース情報を見て、取得したいリソースを指定する。これにより、そのリソースを利用する権利を要求する信号として、リソース利用権発行要求が、移動端末装置１１－２から、親機１２－１およびインターネット２１を介して、本親機である親機１２－２に送信される。

ここで、移動端末装置１１－２は、上述のように、親機１２－２のアドレスを親機１２－１に知らせる。これにより、移動端末装置１１－２は、無線通信可能な親機１２－１とインターネット２１を介して、本親機である親機１２－２と通信が可能になる。

ステップＳ７の処理後は、ステップＳ８に進み、CPU６１は、親機１２－１から、リソースを取得する権利を記載した権利文のデータであるリソース利用権を受信したか否かを判定する。ステップＳ８で、CPU６１は、親機１２－１から権利文を受信したと判定した場合、移動端末装置１１－２は、親機１２－１に接続しているリソースを利用する権利があるので、ステップＳ９に進み、親機１２－１に、受信した権利文とリソース要求信号を送信する。ステップＳ９の処理後は、ステップＳ１０に進み、CPU６１は、リソース要求信号に対応して、親機１２－１から送信されたリソース（を利用するのに必要な情報）を受信し、そのリソースをRAM６３に保持して、処理を終了する。

この場合、移動端末装置１１－２は、本親機でない親機１２－１のリソースを使用することができる。

一方、ステップＳ８で、CPU６１は、親機１２－１から権利文を受信していないと判定した場合、ステップＳ１１に進み、親機１２－２から、親機１２－１を介して、リソースを取得する権利を記載した権利文を発行できないことを示すエラー通知を受信したか否かを判定する。ステップＳ１１で、CPU６１は、親機１２－１からエラー通知を受信していないと判定した場合、ステップＳ８に戻り、上述した処理を繰り返す。

また、ステップＳ１１において、CPU６１は、親機１２－２からエラー通知を受信したと判定した場合、移動端末装置１１－２は、親機１２－１に接続しているリソースを取得する権利がないので、処理を終了する。

図４は、図３のステップＳ２とステップＳ６の共通秘密鍵認証処理を説明するフローチャートである。この処理は、移動端末装置１１とそのユーザの本親機との間で行われる。

図４の例では、移動端末装置１１－１における共通秘密鍵認証処理を説明するが、移動端末装置１１－２における場合も同様の処理が行われる。但し、移動端末装置１１－２の場合は、本親機である親機１２－２と無線通信が可能ではないので、無線通信可能な親機１２－１にその本親機である親機１２－２のアドレス

を通知し、親機１２－１を介して、インターネット２１経由で本親機である親機１２－２と通信する。

ステップＳ２１において、CPU６１は、リーダライタ６５を制御して、非接触ＩＣカード７１から、ユーザの認証情報である共通秘密鍵３１を読み込み、RAM６３に保持する。ステップＳ２１の処理後は、ステップＳ２２に進み、CPU６１は、共通秘密鍵３１を暗号化し、ステップＳ２３に進む。即ち、移動端末装置１１－１は、認証装置１３から親機１２－１（本親機）の秘密鍵３５に対応する公開鍵３９を取得し、RAM６３に保持する。CPU６１は、RAM６３に保持した公開鍵３９を、共通秘密鍵３１とともに暗号/復号部６９に供給する。暗号/復号部６９は、その公開鍵３９を用いて、共通秘密鍵３１を暗号化する。

ステップＳ２３では、CPU６１は、ステップＳ２２で暗号化した共通秘密鍵３１を、本親機である親機１２－１に送信し、ステップＳ２４に進む。ステップＳ２４において、CPU６１は、親機１２－１（本親機）から、後述する図８のステップＳ６４で送信されてくる秘密鍵３５で暗号化された共通秘密鍵３３を受信したかどうかを判定し、暗号化された共通秘密鍵３３を受信していないと判定した場合、受信されるまで待機する。

ステップＳ２４において、CPU６１は、親機１２－１から暗号化された共通秘密鍵３３を受信したと判定した場合、ステップＳ２５に進み、暗号/復号部６９を制御し、その暗号化された共通秘密鍵３３を、ステップＳ２２の処理でRAM６３に保持した、秘密鍵３５と対の公開鍵３９を用いて復号する。このとき、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて生成された暗号文（パスフレーズ）を他方の鍵を用いて復号できる関係にあるので、秘密鍵３５に基づいて暗号化された共通秘密鍵３３（パスフレーズ）が、親機１２－１から送信され、移動端末装置１１－１で受信されるまでの間に改ざんされなかった場合、その暗号化された共通秘密鍵３３は、公開鍵３９に基づいて復号されると、共通秘密鍵３３となる。

ステップＳ２５の処理後は、ステップＳ２６に進み、CPU６１は、暗号/復号部６９を制御して、復号した共通秘密鍵３３を、ステップＳ２２の処理でRAM６３に保持した公開鍵３９を用いて暗号化し、その暗号化した共通秘密鍵を親機１２－１（本親機）に送信し、ステップＳ２７に進む。ステップＳ２７において、CPU６１は、親機１２－１（本親機）から、後述する図８のステップＳ６８の処理で秘密鍵３５を用いて暗号化された共通秘密鍵（親機１２－１が、ステップＳ２３で親機１２－１に送信された暗号化した共通秘密鍵３１を秘密鍵３５を用いて復号し、さらに暗号化した共通秘密鍵）３１を受信したかどうかを判定する。

ステップＳ２７で、CPU６１は、親機１２－１から暗号化された共通秘密鍵３１を受信したと判定した場合、ステップＳ２８に進み、暗号/復号部６９を制御して、その暗号化された共通秘密鍵３１を、秘密鍵３５と対のRAM６３に保持した公開鍵３９を用いて復号する。ステップＳ２８の処理後は、ステップＳ２９に進み、ステップＳ２８で復号された共通秘密鍵が、ステップＳ２１でRAM６３に保持された共通秘密鍵３１と等しいかどうかを判定する。

ステップＳ２９において、CPU６１は、復号された共通秘密鍵３１が、RAM６３に保持された共通秘密鍵３１と等しいと判定した場合、図３のステップＳ３または図３のステップＳ７にリターンする。即ち、この場合、ステップＳ２３で公開鍵３９を用いて暗号化された共通秘密鍵３１が、親機１２－１により秘密鍵３５を用いて正常に復号され、共通秘密鍵３１が得られている。そして、その共通秘密鍵３１が、親機１２－１において秘密鍵３５を用いて暗号化され、その暗号化された共通秘密鍵３１が、移動端末装置１１－１において、公開鍵３９を用いて正常に復号され、共通秘密鍵３１が得られている。

従って、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて暗号化された共通秘密鍵３１を他方の鍵を用いて復号できる関係にあるので、移動端末装置１１－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったことを認識できる。

一方、ステップＳ２９において、CPU６１は、ステップＳ２８で復号された共通秘密鍵が、RAM６３に保持された共通秘密鍵３１と等しくないと判定した場合、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて生成された共通秘密鍵３１を他方の鍵を用いて復号できる関係にないので、移動端末装置１１－１と親機１２－１が通信する間で改ざんがあった、あるいは、親機１２－１が正当な装置でないと認識し、処理を終了する。

このように、移動端末装置１１－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったと認識できたときのみ、図３のステップＳ３または図３のステップＳ７に進み、親機１２－１にリソースを要求する信号を送信するので、移動端末装置１１－１と親機１２－１の両者間での通信中のデータ秘匿が可能となる。

一方、ステップＳ２７において、CPU６１は、親機１２－１から暗号化された共通秘密鍵３１を受信していないと判定した場合、ステップＳ３０に進み、後述する図８のステップＳ７１で親機１２－１が送信した、親機１２－１と移動端末装置１１－１の関係が正当ではないことを示すエラー通知を受信したか否かを判定する。ステップＳ３０において、CPU６１は、親機１２－１からエラー通知を受信していないと判定した場合、ステップＳ２７に戻り、上述した処理を繰り返す。

一方、ステップＳ３０において、CPU６１は、親機１２－１からエラー通知を受信したと判定した場合、親機１２－１と移動端末装置１１－１の関係は正当ではないので、処理を終了する。

図５は、図３のステップＳ５の処理を説明するフローチャートである。

ステップＳ４１において、例えば、移動端末装置１１－２のCPU６１は、直接無線通信することができる本親機でない親機１２－１にデバイス探索を要求する。

ステップＳ４１の処理後は、ステップＳ４２に進み、CPU６１は、親機１２－１から、デバイス探索を許可された（後述する図１２のステップＳ１２１で送信されたデバイス探索許可の通知を受信した）かどうかを判定する。ステップＳ４

２において、CPU６１は、親機１２－１からデバイス探索が許可されたと判定した場合、ステップＳ４３に進み、親機１２－１にリソース情報を要求する。

ステップＳ４３の処理後は、ステップＳ４４に進み、CPU６１は、リソース情報要求に対応して、親機１２－１から送信されたリソース情報を受信し、そのリソース情報をRAM６３に保持する。

一方、ステップＳ４２において、CPU６１は、親機１２－１から、デバイス探索を許可されていないと判定した場合、ステップＳ４５に進み、デバイス探索に対応して親機１２－１から送信されたデバイス探索の不許可を示すエラー通知が、受信されたかどうかを判定する。ステップＳ４５において、CPU６１は、エラー通知が受信されていないと判定した場合、ステップＳ４２に戻り、上述した処理を繰り返す。

また、ステップＳ４５において、CPU６１は、エラー通知が受信されたと判定した場合、親機１２－１にデバイス探索が許可されず、親機１２－１からリソース情報を得ることができないので、処理を終了する。

図６は、図１の親機１２の詳細構成例を示している。

図６の例では、親機１２－１を説明するが、親機１２－２も同様に構成される。

親機１２－１は、CPU９１、ROM９２、RAM９３、アンテナ９４、受信部９５、送信部９６、入出力部９７、データバス９８、リソース制御部９９、および通信部１００から構成されている。

CPU９１は、ROM９２に記憶されているプログラムに従って各種の処理を実行する。例えば、CPU９１は、受信部９５から供給された受信データの供給先を判定し、入出力部９７を制御して、その供給先に、受信データを供給する。RAM９３には、CPU９１が各種の処理を実行する上において必要なデータなどが適宜記憶される。

アンテナ９４は、移動端末装置１１から送信された信号を受信し、その信号を受信部９５に供給する。また、アンテナ９４は、送信部９６から供給された信号を移動端末装置１１に送信する。

受信部９５は、アンテナ９４から供給された信号をCPU９１に供給する。送信部９６は、CPU９１からの指令に基づいて、移動端末装置１１に送信する信号をアンテナ９４に供給する。

入出力部９７は、データバス９８を介してリソース制御部９９と通信部１００に接続されるとともに、リソース機器１６－１とリソース機器１６－２に接続されている。リソース制御部９９は、リソース機器１５－１とリソース機器１５－２にそれぞれ接続されている。

通信部１００は、CPU９１からの指令に基づき、インターンネット２１を介して、親機１２－２、認証装置１３、およびバリュー発行装置１４に信号を送信するとともに、親機１２－２、認証装置１３、およびバリュー発行装置１４から信号を受信する。

図７は、図６のリソース制御部９９の詳細構成例を示している。

リソース制御部９９は、CPU１１１、ROM１１２、RAM１１３、入出力部１１４、リーダライタ１１５、表示部１１６、および暗号/復号部１１７から構成される。

CPU１１１は、ROM１１２に記憶されているプログラムに従って各種の処理を実行する。RAM１１３は、ユーザの個人情報を格納しており、CPU１１１は、個人情報を管理している。また、RAM１１３には、CPU１１１が各種の処理を実行する上において必要なデータなどが適宜記憶される。

CPU１１１は、入出力部１１４を介して、リソース機器１５－１とリソース機器１５－２に接続されており、リソース機器１５－１とリソース機器１５－２から供給されたリソースを、データバス９８および入出力部９７を介して、CPU９１に供給する。リーダライタ１１５は、親機１２－１に備えられた非接触ＩＣカード１２１から、データを読み込んだり、データを書き込む。

非接触ＩＣカード１２１には、個人認証用の情報の格納領域と電子バリューのための認証用の情報の格納領域が設けられている。個人認証用の情報の格納領域には、移動端末装置１１－１の共通秘密鍵３１と同一の共通秘密鍵３３と自らの正当性を証明するための秘密鍵３５が格納されている。電子バリューのための認

証用の情報の格納領域には、バリュー発行装置１４により発行された共通秘密鍵３４等が格納されている。なお、電子バリューのための認証用の情報の格納領域は、認証用と電子バリュー用の領域に分けることができる。認証用の領域には、秘密鍵３４が格納され、電子バリューの領域には、電子バリュー（例えば、権利文）が格納される。

このように、共通秘密鍵３３、共通秘密鍵３４、および秘密鍵３５を改ざんが困難な非接触ＩＣカード１２１に安全に格納することにより、通信システムの安全性と利便性を向上させることができる。

表示部１１６は、CPU１１１の指令により、例えば、リソース情報を表示する。暗号/復号部１１７は、鍵、その他の情報を暗号化または復号する。

なお、親機１２－１は、物理的に１つの筐体で構成する必要はなく、データバスを経由して複数の機器が協調して機能を実現するように構成してもよい。

図８は、図７の親機１２のリソース制御部９９がリソースを制御する処理を説明するフローチャートである。この処理は、例えば、移動端末装置１１から信号を受信したとき開始される。

以下の説明では、親機１２－１がリソースを制御する処理を説明するが、親機１２－２における場合も同様の処理が行われる。

ステップＳ６１では、CPU１１１は、リーダライタ１１５を制御し、非接触ＩＣカード１２１から共通秘密鍵３３を読み込み、その共通秘密鍵３３をRAM１１３に保持する。ステップＳ６１の処理後は、ステップＳ６２に進み、CPU１１１は、図４のステップＳ２３で移動端末装置１１－１から送信された暗号化した共通秘密鍵３１が受信されたかどうかを判定する。

即ち、CPU９１は、アンテナ９４により受信され、受信部９５を介して供給された信号が、親機１２－１に対するものである場合、入出力部９７を制御し、データバス９８を介して、その信号をリソース制御部９９のCPU１１１に供給し、CPU１１１は、その信号が暗号化された共通秘密鍵３１であるかどうかを判定する。なお、以下の説明では、このようにCPU９１がアンテナ９４により受信され

た信号をリソース制御部９９のCPU１１１に供給することを、単に、CPU１１１が信号を受信するという。

ステップＳ６２において、CPU１１１は、移動端末装置１１－１から暗号化された共通秘密鍵３１が受信されたと判定した場合、ステップＳ６３に進み、非接触ＩＣカード１２１から秘密鍵３５を読み込み、その暗号化された共通秘密鍵３１と秘密鍵３５をRAM１１３に保持する。そして、CPU１１１は、暗号/復号部１１７を制御し、ステップＳ６１でRAM１１３に保持した共通秘密鍵３３を、秘密鍵３５を用いて暗号化する。

ステップＳ６３の処理後は、ステップＳ６４に進み、CPU１１１は、ステップＳ６２で暗号化された共通秘密鍵３３を、移動端末装置１１－１に送信し、ステップＳ６４からステップＳ６５に進む。ステップＳ６５では、CPU１１１は、図４のステップＳ２６で移動端末装置１１－１から送信された暗号化された共通秘密鍵が受信されたかどうかを判定し、移動端末装置１１－１から暗号化された共通秘密鍵が受信されるまで待機する。

ステップＳ６５において、CPU１１１は、移動端末装置１１－１から暗号化された共通秘密鍵が供給されたと判定した場合、ステップＳ６６に進み、その暗号化された共通秘密鍵を復号し、ステップＳ６７に進む。即ち、CPU１１１は、暗号/復号部１１７を制御し、ステップＳ６３でRAM１１３に保持した、公開鍵３９と対の秘密鍵３５を用いて、暗号化された共通秘密鍵を復号する。

ステップＳ６７では、CPU１１１は、その復号された共通秘密鍵が、RAM１１３に保持された共通秘密鍵３３と等しいかどうかを判定する。ステップＳ６７において、CPU１１１は、その復号された共通秘密鍵がRAM１１３に保持された共通秘密鍵３３と等しいと判定した場合、ステップＳ６８に進む。

即ち、この場合、ステップＳ６３で秘密鍵３５を用いて暗号化された共通秘密鍵３３が、移動端末装置１１－１において、公開鍵３９を用いて正常に復号され、共通秘密鍵３３が得られている。そして、その秘密鍵３３が移動端末装置１１－１において、公開鍵３９を用いて暗号化され、その暗号化されたた共通秘密鍵３

１が、親機１２－１において、秘密鍵３５を用いて正常に復号され、共通秘密鍵３３が得られている。

従って、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて暗号化された共通秘密鍵３３を他方の鍵を用いて復号できる関係にあるので、親機１２－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったことが認識できる。

その後、ステップＳ６８において、CPU１１１は、ステップＳ６２で移動端末装置１１－１から受信し、RAM１１３に保持した暗号化された共通秘密鍵３１を、RAM１１３に保持した公開鍵３９と対の秘密鍵３５を用いて復号する。

ステップＳ６８の処理後は、ステップＳ６９に進み、CPU１１１は、ステップＳ６８で復号した共通秘密鍵が、RAM１１３に保持した共通秘密鍵３３と等しいかどうかを判定する。ステップＳ６９において、CPU１１１は、その復号した共通秘密鍵がRAM１１３に保持した共通秘密鍵３３と等しいと判定した場合、ステップＳ７０に進む。

即ち、この場合、図４のステップＳ２２で移動端末装置１１－１により公開鍵３９を用いて暗号化された、秘密鍵３３と同一の共通秘密鍵３１が、ステップＳ６８で親機１２－１により秘密鍵３５を用いて正常に復号され、共通秘密鍵３１が得られている。そして、移動端末装置１１－１が有する共通秘密鍵３１と親機１２-１が有する共通秘密鍵３３が同一であることが検証、つまり、移動端末装置１１－１のユーザが、親機１２－１のユーザであることが検証されている。

従って、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて暗号化された共通秘密鍵３１を他方の鍵を用いて復号できる関係にあるので、親機１２－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったことが認識できる。また、移動端末装置１１－１が有する共通秘密鍵３１と親機１２－１が有する共通秘密鍵３３が等しくなっているので、親機１２－１は、移動端末装置１１－１のユーザが個人情報を格納したユーザであることを認識する。

その後、ステップＳ７０において、暗号/復号部６９を制御して、その復号した共通秘密鍵を、RAM１１３に保持した秘密鍵３５を用いて暗号化し、移動端末装置１１－１に送信する。

一方、ステップＳ６７において、CPU１１１は、ステップＳ６６で復号された共通秘密鍵が RAM１１３に保持する共通秘密鍵３３と等しくないと判定した場合、またはステップＳ６９で、ステップＳ６８で復号された共通秘密鍵が RAM１１３に保持する共通秘密鍵３３と等しくないと判定した場合、移動端末装置１１－１と親機１２－１が通信する間で改ざんがあったか、または親機１２－１が移動端末装置１１－１の本親機ではないので、ステップＳ７１に進み、移動端末装置１１－１と親機１２－１の関係が正当ではないことを示すエラー通知を送信し、処理を終了する。

このように、親機１２－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなく、かつ移動端末装置１１－１の本親機であると認識できたときのみ、復号した共通秘密鍵３１を暗号化して移動端末装置１１－１に送信する。

この後、移動端末装置１１－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったと認識できたときのみリソースを要求する信号を親機１２－１に送信するので、移動端末装置１１－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったと移動端末装置１１－１と親機１２－１の両者で認識（双方向認証）され、かつ親機１２－１が移動端末装置１１－１の本親機である場合のみ、リソースを要求し、利用することができる。

これにより、移動端末装置１１－１と親機１２－１の両者間での通信中のデータ秘匿が可能となる。

ステップＳ６２において、CPU１１１は、移動端末装置１１－１からリソース要求信号が供給されたと判定した場合、ステップＳ７３に進み、リソース送信処理を行い、その後、処理を終了する。リソース送信処理の詳細は、図９と図１０で後述する。

一方、ステップＳ７２において、CPU１１１は、リソース要求信号が供給されていないと判定した場合、ステップＳ６２に戻り、上述した処理を繰り返す。

図９は、移動端末装置１１－１および１１－２と直接無線通信が可能な親機１２－１が図８のステップＳ７３の処理で行うリソース送信処理を説明するフローチャートである。

ステップＳ８１において、親機１２－１のCPU１１１は、図８のステップＳ７２で受信したリソース要求信号が自身が本親機となる移動端末装置（移動端末装置１１－１）からのリソース要求信号であるかどうかを判定する。ステップＳ８１において、親機１２－１のCPU１１１は、受信したリソース要求信号が自身が本親機となる移動端末装置１１－１からのリソース要求信号であると判定した場合、ステップＳ８２をスキップしてステップＳ８３に進む。

ステップＳ８３では、親機１２－１のCPU１１１は、入出力部１１４を制御し、移動端末装置１１－１からのリソース要求信号に基づいて、移動端末装置１１－１から要求されているリソースを有するリソース機器１５からリソースを取得し、ステップＳ８４に進む。ステップＳ８４では、親機１２－１のCPU１１１は、そのリソースを、移動端末装置１１－１に送信してリターンする。

即ち、親機１２－１は、個人情報を格納しているユーザが使用する移動端末装置１１－１から、親機１２－１の接続するリソース機器１５の有するリソースを要求された場合、無条件に利用を許可する。

一方、ステップＳ８１において、親機１２－１のCPU１１１は、図８のステップＳ７２で受信したリソース要求信号が、自身が本親機とならない移動端末装置からのリソース要求信号である（移動端末装置１１－２からのリソース要求信号である）と判定した場合、ステップＳ８２に進み、権利文の提示がある（リソース要求信号とともに権利文が送信されてきた）かどうかを判定する。ステップＳ８２において、親機１２－１のCPU１１１は、権利文の提示がなかったと判定した場合、移動端末装置１１－２はリソースを利用する権利がないので、処理を終了する。

ステップＳ８２において、親機１２－１のCPU１１１は、権利文の提示があったと判定した場合、ステップＳ８３に進み、入出力部１１４を制御し、移動端末装置１１－２からのリソース要求信号に基づいて、移動端末装置１１－２から要求されているリソースを有するリソース機器１５からリソースを取得し、ステップＳ８４に進む。ステップＳ８４では、親機１２－１のCPU１１１は、そのリソースを、移動端末装置１１－２に送信する。

即ち、親機１２－１は、個人情報を格納していないユーザが使用する移動端末装置１１－２から、親機１２－１に接続しているリソース機器１５の有するリソースを要求された場合、移動端末装置１１－２がリソースを利用する権利文を取得している場合のみ、リソース利用を許可する。逆に言えば、移動端末装置１１－２のユーザは、本親機１２－１のリソースを、そのリソースを利用する権利文を、親機１２－１に提示したときのみ利用することができる。

なお、親機１２－１は、親機１２－２が移動端末装置１１－２のユーザを認証するときのやりとり時に、移動端末装置１１－２は、そのユーザの個人情報を、その本親機である親機１２－２から取得する。ここで、個人情報には、そのユーザがリソースを利用したときの操作履歴などが含まれる。即ち、移動端末装置１１－２の本親機である親機１２－２は、例えば、そのユーザが自身の有するリソースを利用したときに、その利用時の操作履歴などを個人情報として登録する個人情報管理機能を有する。移動端末装置１１－２は、親機１２－１のリソースを利用するときに、ユーザの個人情報に応じて、移動端末装置１１－２のユーザの嗜好に合わせた操作性（ユーザＩ／Ｆ）を提供する。

図１０は、移動端末装置１１－２がその本親機である親機１２－２と直接無線通信できない場合に、その親機１２－２が図８のステップＳ７１の処理で行うリソース送信処理を説明するフローチャートである。なお、親機１２－２は、認証装置１３から発行された電子証明書（図１１で後述する）を既に受信し、RAM１１３に保持しているものとする。

ステップＳ１００において、親機１２－２のCPU１１１は、暗号化した利用権発行要求文と、RAM１１３に保持している電子証明書を作成し、その利用権発行要求文と電子証明書を、移動端末装置１１－１がリソースを利用しようとする本親機でない親機１２－１に送信する。即ち、親機１２－２のCPU１１１は、直接無線通信することができない移動端末装置１１－２から送信されたリソース要求信号に基づいて、リソース情報の識別子と利用方法を明記した利用権発行要求文を作成する。

また、親機１２－２のCPU１１１は、リーダライタ１１５を制御し、非接触ＩＣカード１２１から読み込んだ秘密鍵３８をRAM１１３に保持する。CPU１１１は、暗号/復号部１１７を制御し、RAM１１３に保持した秘密鍵３８を用いて、電子署名を暗号化し、利用権発行要求文を付加する。そして、CPU１１１は、その利用権発行要求文を電子証明書とともに、移動端末装置１１－２がリソースを利用しようとしている親機１２－１に送信する。

なお、利用権発行要求文とは、ここでは、移動端末装置１１－２が、その本親機でない親機１２－１のリソースの利用をするための利用権の発行を、親機１２－１に要求するメッセージである。

また、移動端末装置１１－２が本親機である親機１２－２に送信するリソース要求信号には、その移動端末装置１１－２がリソースを利用しようとする本親機でない親機１２－２へアクセスするためのアクセス情報が含まれている。そして、親機１２－２は、このアクセス情報に基づいて、利用権発行要求文を親機１２－１に送信する。

ステップＳ１００の処理後は、ステップＳ１０１に進み、親機１２－２のCPU１１１は、後述する図１３のステップＳ１４７で、利用権発行要求文を受信した親機１２－１が親機１２－２に対して送信するリソースの利用を許可するための対価（バリュー）と対価の送信先口座情報を記載したリソース利用条件文と電子証明書を受信したかどうかを判定する。ステップＳ１０１において、親機１２－２のCPU１１１は、リソース利用条件文と電子証明書を受信したと判定した場合、

暗号/復号部１１７を制御し、電子証明書に含まれる、親機１２－１の秘密鍵３５に対応する公開鍵３９を用いて、リソース利用条件文に含まれる電子署名を復号し、ステップＳ１０１からステップＳ１０２に進む。

ステップＳ１０２において、親機１２－２のCPU１１１は、リソース利用条件文が正当であるかどうかを判定する。即ち、CPU１１１は、リソース利用条件文に含まれる電子署名が正常に復号されたかどうかを判定する。ステップＳ１０２において、CPU１１１は、リソース利用条件文が正当ではないと判定した場合、親機１２－１の秘密鍵３５で暗号化された電子署名が、それと対の公開鍵３９で復号できていないので、親機１２－１と親機１２－２が通信する間で改ざんが行われたと判定し、処理を終了する。

また、ステップＳ１０２において、親機１２－２のCPU１１１は、リソース利用条件文が正当であると判定した場合、秘密鍵３５で暗号化された電子署名が、公開鍵３９で復号できるので、親機１２－１と親機１２－２が通信する間で改ざんが行われず、親機１２－１と親機１２－２が正当な関係であると認識し、ステップＳ１０２からステップＳ１０３に進む。

このように、電子署名を用いてリソース利用条件文が正当であるかどうかを判定することにより、通信システム１の安全性をさらに高めることができる。

ステップＳ１０３において、親機１２－２のCPU１１１は、リソース利用条件文に基づいて、親機１２－２から親機１２－１にバリューを移動する（対価を支払う）ためのバリュー移動要求をバリュー発行装置１４に送信する。

ステップＳ１０３の処理後は、ステップＳ１０４に進み、親機１２－２のCPU１１１は、バリュー発行装置１４から、後述する図１６のステップＳ１６２で送信される暗号化された共通秘密鍵４４を受信したかどうかを判定する。ステップＳ１０４において、CPU１１１は、バリュー発行装置１４から暗号化された共通秘密鍵４４を受信していないと判定した場合、バリュー発行装置１４から暗号化された共通秘密鍵４４が受信されるまで待機する。

ステップＳ１０４において、親機１２－２のCPU１１１は、バリュー発行装置１４から暗号化された共通秘密鍵４４を受信したと判定した場合、ステップＳ１０５に進み、親機１２－２のCPU１１１は、バリュー発行装置１４の有する秘密鍵４３に対応する公開鍵４１を、認証装置１３から取得し、RAM１１３に保持する。そして、親機１２－２のCPU１１１は、暗号/復号部１１７を制御し、RAM１１３に保持した公開鍵４１を用いて、暗号化された共通秘密鍵４４を復号し、復号した共通秘密鍵４４をRAM１１３に保持する。

ステップＳ１０５の処理後は、ステップＳ１０６に進み、親機１２－２のCPU１１１は、リーダライタ１１５を制御して、共通秘密鍵３７を読み込み、RAM１１３に保持し、ステップＳ１０７に進む。ステップＳ１０７では、親機１２－２のCPU１１１は、RAM１１３から復号した共通秘密鍵４４と共通秘密鍵３７を読み出し、両者が等しいかどうかを判定する。

ステップＳ１０７において、親機１２－２のCPU１１１は、復号した共通秘密鍵４４と共通秘密鍵３７が等しいと判定した場合、即ち、後述する図１６のステップＳ１６１でバリュー発行装置１４により秘密鍵４３を用いて暗号化された共通秘密鍵４４が、ステップＳ１０６で親機１２－２により公開鍵４１を用いて正常に復号され、共通秘密鍵３７と等しい共通秘密鍵４４が得られている場合、親機１２－２のCPU１１１は、バリュー発行装置１４と親機１２－２が通信する間で改ざんがなかったことが認識し、ステップＳ１０７からステップＳ１０８に進む。

従って、CPU１１１は、Ｓ１０８では、親機１２－２のCPU１１１は、暗号/復号部１１７を制御し、RAM１１３に保持した公開鍵４１を用いて、RAM１１３に保持した共通秘密鍵３７を暗号化する。ステップＳ１０９の処理後は、ステップＳ１１０に進み、親機１２－２のCPU１１１は、その暗号化した共通秘密鍵３７を、バリュー発行装置１４に送信し、リターンする。

一方、ステップＳ１０７において、親機１２－２のＣＰＵ１１１は、ステップＳ１０６で復号した共通秘密鍵と共通秘密鍵３４が等しくないと判定した場合、

バリュー発行装置１４と親機１２－２が通信する間で改ざんがあったと認識し、ステップＳ１１０に進み、バリュー発行装置１４に、バリュー発行装置１４と親機１２－２の関係は正当ではないことを示すエラーを通知してリターンする。

また、ステップＳ１０１において、親機１２－２のCPU１１１は、移動端末装置１２－２がリソースを利用しようとする親機１２－１からのリソース利用条件文を受信していないと判定した場合、ステップＳ１１１に進み、親機１２－１から、後述する図１３のステップＳ１４８で送信されたるリソース利用条件文を発行できないことを示すエラー通知を受信したかどうかを判定する。ステップＳ１１０において、親機１２－２のCPU１１１は、親機１２－１からエラー通知を受信していないと判定した場合、ステップＳ１０１に戻り、上述した処理を繰り返す。

また、ステップＳ１１１において、親機１２－２のCPU１１１は、親機１２－１からエラー通知を受信したと判定した場合、即ち、親機１２－１がリソース利用条件文を発行せず、移動端末装置１１－２によるリース利用を許可しなかった場合、処理を終了する。

図１１は、電子証明書の例を示す図である。

この電子証明書は、図１１に示されるように、証明書のバージョン番号、証明書の通し番号、署名に用いたアルゴリズムとパラメータ、認証装置１３の名前、証明書の有効期限、発行された装置のＩＤ、および装置の公開鍵が含まれている。

この電子証明書は、認証装置１３により、親機１２－１、親機１２－２、およびバリュー発行装置１４に対して発行される。親機１２－１、親機１２－２、およびバリュー発行装置１４は、自らの正当性を証明するために他の装置に、暗号文とともにこの電子証明書を送信する。受信した装置は、この電子証明書に含まれる装置の公開鍵を用いて、この電子証明書とともに送信されてくる暗号文を復号し、その暗号文の正当性を認識することができる。

図１２は、図６の親機１２－１がリソース情報を送信する処理を説明するフローチャートである。この処理は、例えば、親機１２－１が図５のステップＳ４１

で移動端末装置１１－２から送信されるブロードキャスト要求信号を受信したとき開始される。

ステップＳ１２０において、親機１２－１のCPU９１は、移動端末装置１１－２によるブロードキャスト要求を許可するかどうかを判定する。ステップＳ１２０において、親機１２－１のCPU９１は、ブロードキャスト要求を許可すると判定した場合、ステップＳ１２１に進み、移動端末装置１１－２にブロードキャスト要求許可の通知を送信する。

ステップＳ１２１の処理後は、ステップＳ１２２に進み、親機１２－１のCPU９１は、移動端末装置１１－２から図５のステップＳ４３でリソース情報要求信号が送信されて来るのを待って受信し、ステップＳ１２３に進む。

ステップＳ１２３において、親機１２－１のCPU９１は、入出力部９７を制御し、データバス９８とリソース制御部９９を介して、リソース機器１５－１とリソース機器１５－２から、移動端末装置１２－２に提供することができる、または提供してもよいリソースのリソース情報を取得する。同様に、CPU９１は、入出力部９７を制御し、データバス９８を介して、リソース機器１６－１とリソース機器１６－２からリソース情報を取得する。そして、CPU９１は、取得したリソース情報を移動端末装置１１－２に送信して処理を終了する。

一方、ステップＳ１２０において、CPU９１は、移動端末装置１１－２からのブロードキャスト要求を許可しないと判定した場合、ステップＳ１２４に進み、移動端末装置１１にブロードキャスト要求を許可しないことを示すエラー通知を送信し、処理を終了する。

図１３は、図６の親機１２－１が、リソース利用条件文を発行するときに行うリソース利用条件文発行処理を説明するフローチャートである。この処理は、親機１２－１が図１０のステップＳ１００の処理で親機１２－２から送信された、暗号化された利用権発行要求文と電子証明書を受信したとき開始される。なお、親機１２－１は、認証装置１３から発行された電子証明書（図１１）を既に受信し、RAM１１３に保持しているものとする。

ステップＳ１４１において、親機１２－１のCPU１１１は、親機１２－２から利用権発行要求文とともに受信した電子証明書から公開鍵４０を取得し、ステップＳ１４２に進む。ステップＳ１４２では、親機１２－１のCPU１１１は、親機１２－２から受信した利用権発行要求文から秘密鍵３８を用いて暗号化された電子署名を取得する。CPU１１１は、暗号/復号部１１７を制御して、電子署名を、ステップＳ１４１で取得した、秘密鍵３８と対の公開鍵４０を用いて復号する。

ステップＳ１４２の処理後は、ステップＳ１４３に進み、親機１２－１のCPU１１１は、利用権発行要求文が正当であるかどうかを判定する。即ち、親機１２－１のCPU１１１は、ステップＳ１４２で電子署名が正常に復号されたかどうかを判定し、電子署名が正常に復号された場合、秘密鍵３８で暗号化された電子署名が、秘密鍵３８に対応する公開鍵４０で正常に復号されているので、親機１２－１と親機１２－２が通信する間で改ざんが行われていないと認識し、利用権発行要求文が正当であると判定する。

ステップＳ１４３において、親機１２－１のCPU１１１は、利用権発行要求文が正当ではないと判定した場合、リソース利用を許可することはできないので、ステップＳ１４８に進み、リソース利用の不許可を示すエラー通知を送信して処理を終了する。

ステップＳ１４３において、親機１２－１のCPU１１１は、利用権発行要求文が正当であると判定した場合、ステップＳ１４４に進み、親機１２－２から受信した電子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装置１３に送信し、ステップＳ１４５に進む。

ステップＳ１４５では、親機１２－１のCPU１１１は、認証装置１３から、図１８のステップＳ１８３またはステップＳ１８４で送信される電子証明書の評価を受信したかどうかを判定し、電子証明書の評価を受信していないと判定した場合、電子証明書の評価を受信するまで待機する。

ステップＳ１４５において、親機１２－１のCPU１１１は、認証装置１３から電子証明書の対価を受信したと判定した場合、ステップＳ１４６に進み、その認

証装置１３からの電子証明書の評価が有効であるかどうかを判定する。ステップＳ１４６において、親機１２－１のCPU１１１は、認証装置１３から電子証明書は有効であるという評価を受信したと判定した場合、即ち、利用件発行要求とともに送信されてきた電子証明書が失効していない（無効でない）場合、ステップＳ１４７に進み、リソース利用を許可するための対価を記載したリソース利用条件文を電子的に作成する。

このとき、親機１２－１のCPU１１１は、暗号/復号部１１７を制御して、自らの正当性を証明するために、秘密鍵３５を用いて電子署名を暗号化し、リソース利用条件文に電子署名を付加する。そして、CPU１１１は、電子署名を付加した利用条件文と、RAM１１３に保持した電子証明書を、親機１２－２に送信し、処理を終了する。

一方、ステップＳ１４６において、親機１２－１のCPU１１１は、認証装置１３から電子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース利用を許可することはできないので、ステップＳ１４８に進み、リソース利用の不許可を示すエラー通知を親機１２－２に送信し、処理を終了する。

なお、親機１２－１がリソースを利用する権利を記載した権利文を発行する処理も、図１３と同様にして行われる。但し、この権利文を発行する処理は、バリュー発行装置１４から、後述する図１６のステップＳ１６８で送信される暗号化された振込み通知書と電子証明書を受信したとき開始される。

即ち、図１４は、図６の親機１２－１がリソースを利用するための権利文を発行するときに行う権利文発行処理を説明するフローチャートである。この処理は、親機１２－１が後述する図１６のステップＳ１６８の処理でバリュー発行装置１４から送信される、振込み通知書と電子証明書を受信したとき開始される。なお、親機１２－１は、認証装置１３から発行された電子証明書（図１１）を既に受信し、RAM１１３に保持しているものとする。

ステップＳ１５１において、親機１２－１のCPU１１１は、バリュー発行装置１４から、振り込み通知書とともに受信した電子証明書から公開鍵４１を取得し、ステップＳ１５２に進む。ステップＳ１５２では、親機１２－１のCPU１１１は、バリュー発行装置１４から受信した振込み通知書から秘密鍵４３を用いて暗号化された電子署名を取得する。親機１２－１のCPU１１１は、暗号/復号部１１７を制御して、電子署名を、ステップＳ１５１で取得した公開鍵４１を用いて復号する。

ステップＳ１５２の処理後は、ステップＳ１５３に進み、親機１２－１のCPU１１１は、振込み通知書が正当であるかどうかを判定する。即ち、CPU１１１は、電子署名が正常に復号されたかどうかを判定し、電子署名が正常に復号された場合、秘密鍵４３で暗号化された電子署名が、秘密鍵４３に対応する公開鍵４１で正常に復号されているので、親機１２－１とバリュー発行装置１４が通信する間で改ざんが行われていないと認識し、振込み通知書が正当であると判定する。

ステップＳ１５３において、親機１２－１のCPU１１１は、振込み通知書が正当ではないと判定した場合、リソース利用を許可することはできないので、ステップＳ１５８に進み、リソース利用の不許可を示すエラー通知を送信して処理を終了する。

また、ステップＳ１５３において、親機１２－１のCPU１１１は、振込み通知書が正当であると判定した場合、ステップＳ１５４に進み、バリュー発行装置１４から受信した電子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装置１３に送信し、ステップＳ１５５に進む。

ステップＳ１５５では、親機１２－１のCPU１１１は、認証装置１３から、後述する図１８のステップＳ１８３またはステップＳ１８４で送信される電子証明書の評価を受信したかどうかを判定し、電子証明書の評価を受信していないと判定した場合、電子証明書の評価を受信するまで待機する。

そして、ステップＳ１５５において、親機１２－１のCPU１１１は、認証装置１３から電子証明書の評価を受信したと判定した場合、ステップＳ１５６に進み、

CPU１１１は、認証装置１３から電子証明書は有効であるという評価を受信したかどうかを判定する。ステップＳ１５６において、CPU１１１は、認証装置１３から電子証明書は有効であるという評価を受信したと判定した場合、ステップＳ１５７に進み、リソースを利用する権利を記載した権利文を電子的に作成する。このとき、親機１２－１のCPU１１１は、暗号/復号部１１７を制御して、自らの正当性を証明するために、秘密鍵３５を用いて電子署名を暗号化し、権利文に電子署名を付加する。そして、親機１２－１のCPU１１１は、電子署名を付加した権利文と、RAM１１３に保持した電子証明書を、親機１２－２に送信して処理を終了する。

一方、ステップＳ１５６において、親機１２－１のCPU１１１は、認証装置１３から電子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース利用を許可することはできないので、ステップＳ１５８に進み、リソース利用の不許可を示すエラー通知を親機１２－２に送信して処理を終了する。

図１５は、図１のバリュー発行装置１４の詳細構成例である。

バリュー発行装置１４は、通信部１３１、データバス１３２、共通秘密鍵認証部１３３、公開鍵認証部１３４、バリュー発行部１３５、共通秘密鍵記憶部１３６、秘密鍵記憶部１３７、証明書記憶部１３８、発行履歴記憶部１３９、およびバリュー記憶部１４０から構成されている。

通信部１３１は、インターネット21を介して、親機１２－１、親機１２－２、および認証装置１３からの信号を受信するとともに、親機１２－１、親機１２－２、および認証装置１３に信号を送信する。通信部１３１は、データバス１３２を介して、共通秘密鍵認証部１３３、公開鍵認証部１３４、およびバリュー発行部１３５に接続されている。

共通秘密鍵認証部１３３は、共通秘密鍵記憶部１３６に記憶された共通秘密鍵４４に基づいて、バリュー発行装置１４にアクセスしてきた親機１２が正当であるかどうかを判定する。また、共通秘密鍵認証部１３３は、バリュー発行装置１

４がバリューを管理する親機１２に対して、共通秘密鍵４４と同一の秘密鍵３４または３７を送信し、親機１２の非接触ＩＣカード１２１に記憶させる。

このように、親機１２の非接触ＩＣカード１２１にバリュー発行装置１４の共通秘密鍵４４と等しい共通秘密鍵３４または３７を記憶させることにより、親機１２とバリュー発行装置１４との間での認証が可能となり、ユーザが、その親機１２と通信が可能な移動端末装置１１を使用するだけで、バリュー発行装置１４を介して、親機１２どうしの間でのバリューの移動をすることができる。

公開鍵認証部１３４は、秘密鍵記憶部１３７に記憶された秘密鍵４３や、証明書記憶部１３８に記憶された電子証明書を用いて、親機１２－１、親機１２－２、および認証装置１３との間で通信部１３１を開始、公開鍵暗号系の処理を行なう。

バリュー発行部１３５は、バリュー記憶部１４０に記憶されたバリュー（電子バリュー）に基づき、バリューを発行し、その発行履歴を発行履歴記憶部１３９に記憶させる。

なお、バリュー発行装置１４は、物理的に１つの筐体に入る必要はなく、データバス１３２を経由して複数の機器が協調して機能を実現してもよい。

また、バリュー発行装置１４は、発行したバリューに応じた対価を決済できるようにしてもよい。さらに、親機１２は、所有する電子バリューをネットワークでの決済に使用してもよい。

また、電子バリューの形式は何でもよい。電子バリューはバリュー発行装置１４のバリュー記憶部１４０に口座という形で格納してもよい。この場合、より高い安全性を提供することができる。

口座を表すＩＤは、親機の証明書にある機器ＩＤ、あるいはそれに対応させた別のＩＤを用いることにより、ユーザは個人情報に結びつかない匿名性の高い口座を持つことができる。

さらに、バリューは、バリュー発行装置１４のバリュー記憶部１４０に口座という形で記憶されるだけでなく、親機１２の安全なデバイス（例えば、非接触ＩＣカード１２１）の記憶領域へ格納されてもよい。この場合、バリュー発行装置

１４のバリュー発行部１３５で発行された電子バリューは、親機１２の非接触ＩＣカード１２１に転送される。例えば、バリュー発行装置１４が、親機１２－２から親機１２－１に対してバリューを振り込む場合、バリュー発行装置１４は、親機１２－２からバリューを取得し、バリューを親機１２－１に送信する。なお、バリューの送受信は、バリューを暗号化して安全に行われる。

また、バリューは、バリュー発行装置１４のバリュー記憶部１４０および親機１２の安全なデバイスの両者の組み合わせによって記憶されてもよい。この組み合わせとして、バリュー発行装置１４は、ユーザの電子バリューをバリュー記憶部１４０の中でそれぞれのユーザの口座として記憶し、その口座を管理しつつ、必要な額だけをユーザのデバイス（例えば、非接触ＩＣカード）へ移動させ財布のように利用させてもよい。

図１６は、図１５のバリュー発行装置１４が振り込み通知書を親機１２－１に送信する処理を説明するフローチャートである。この処理は、バリュー発行装置１４が、親機１２－２が図１０のステップＳ１０３で送信したバリュー移動要求を受信したとき開始される。なお、バリュー発行装置１４は、認証装置１３が発行した電子証明書を、既に証明書記憶部１３８に記憶しているものとする。

ステップＳ１６１において、共通秘密鍵認証部１３３は、共通秘密鍵記憶部１３６から共通秘密鍵４４と、秘密鍵記憶部１３７から秘密鍵４３を読み出し、秘密鍵４３を用いて、共通秘密鍵４４を暗号化する。ステップＳ１６１の処理後は、ステップＳ１６２に進み、共通秘密鍵認証部１３３は、その暗号化された共通秘密鍵４４を親機１２－２に送信し、ステップＳ１６３に進む。即ち、共通秘密鍵認証部１３３は、暗号化された共通秘密鍵４４を、データバス１３２を介して通信部１３１に供給し、通信部１３１は、その暗号化された共通秘密鍵４４を親機１２－２に送信する。

ステップＳ１６３において、通信部１３１は、親機１２－２から、図１０のステップＳ１０９で送信された暗号化された共通秘密鍵３７を受信したかどうかを判定する。ステップＳ１６３において、通信部１３１は、親機１２－２から暗号

化された共通秘密鍵３７を受信していないと判定した場合、ステップＳ１６４に進み、親機１２－２から、図１０のステップＳ１１０で送信される、バリュー発行装置１４と親機１２－２の関係が正当ではないことを示すエラー通知を受信したかどうかを判定する。ステップＳ１６８において、通信部１３１は、エラー通知を受信していないと判定した場合、ステップＳ１６３に戻り、上述した処理を繰り返す。

ステップＳ１６４において、通信部１３１は、エラー通知を受信したと判定した場合、バリュー発行装置１４と親機１２－２の関係が正当ではないので、バリュー移動の不許可を示すエラー通知を送信して処理を終了する。

一方、ステップＳ１６３において、通信部１３１は、親機１２－２から暗号化された共通秘密鍵３７を受信したと判定した場合、その暗号化された共通秘密鍵３７を公開鍵認証部１３４に供給し、ステップＳ１６３からステップＳ１６５に進む。ステップＳ１６５において、公開鍵認証部１３４は、暗号化された共通秘密鍵３７を、秘密鍵記憶部１３７に記憶している秘密鍵４３を用いて復号する。

ステップＳ１６５の処理後は、ステップＳ１６６に進み、公開鍵認証部１３４は、共通秘密鍵認証部１３３に、ステップＳ１６５で復号した共通秘密鍵３７を供給し、共通秘密鍵認証部１３３は、復号した共通秘密鍵３７と共通秘密鍵記憶部１３６に記憶している共通秘密鍵４４が等しいかどうかを判定する。

ステップＳ１６６において、共通秘密鍵認証部１３３は、復号した共通秘密鍵３７と共通秘密鍵４４が等しいと判定した場合、親機１２－２とバリュー発行装置１４の関係は正当であると認識して、ステップＳ１６６からステップＳ１６７に進む。即ち、この場合、親機１２－１において公開鍵４１を用いて暗号化された共通秘密鍵３７が、バリュー発行装置１４において、公開鍵４１に対応する秘密鍵４３を用いて正常に復号され、共通秘密鍵３７が得られているので、バリュー発行装置１４は、親機１２－２とバリュー発行装置１４が通信する間で改ざんが行われていないと認識する。

さらに、バリュー発行装置１４は、親機１２－２が有する共通秘密鍵３７とバリュー発行装置１４が有する共通秘密鍵４４が等しいので、親機１２－２がバリューを管理することを認められている相手であることを認識する。即ち、バリュー発行装置１４は、バリュー発行装置１４の有する共通秘密鍵４４と同一の秘密鍵３７を、親機１２－２に備えられる安全なデバイス（非接触ＩＣカード１２１）に配布し、親機１２－２が共通秘密鍵４４と等しい共通秘密鍵３７を有することを認識することによって、正しい親機１２－２からのアクセスであることを認識する。

ステップＳ１６７において、バリュー発行部１３５は、親機１２－２から親機１２－１にバリューを移動する。即ち、バリュー発行部１３５は、バリュー記憶部１４０に記憶された親機１２－２の所定の対価に対応するバリューを削除し、親機１２－１のバリューに所定の対価に対応するバリューを追加し、これにより、親機１２－２のユーザの電子バリューが、そのユーザが移動端末装置１１－２によってリソースを利用しようとしている親機１２－１のユーザに対し、そのリソースの利用に対する対価として振り込まれる。さらに、ステップＳ１６７では、バリュー発行部１３５は、バリューの移動完了を示す取引結果通知を生成する。

これにより、ユーザは、バリュー発行装置１４を経由して、他のユーザとの間で、電子バリューの授受を行うことができる。

ステップＳ１６７の処理後は、ステップＳ１６８に進み、公開鍵認証部１３４は、秘密鍵記憶部１３７に記憶された秘密鍵４３を用いて、自らの正当性を証明するために電子署名を暗号化する。そして、公開鍵認証部１３４は、その暗号化した電子署名を付加した振込み通知書を作成する。この振込み通知書は、バリューの振込みを知らせるための振込み通知と、バリューの振込みの詳細が記載されたレシートから構成されている。そして、公開鍵認証部１３４は、その振込み通知書、証明書記憶部１３８に記憶された電子証明書、および電子バリューの移動完了を示す取引結果通知を、バリューの振込先であるユーザの親機１２－１に送信して処理を終了する。

一方、ステップＳ１６６において、共通秘密鍵認証部１３３は、ステップＳ１６５で復号した共通秘密鍵と共通秘密鍵４４が等しくないと判定した場合、親機１２－２とバリュー発行装置１４の関係は正当ではないので、バリュー移動の不許可を示すエラー通知を送信して処理を終了する。

図１７は、図１の認証装置１３の詳細構成例を示している。

認証装置１３は、通信部１５１、データバス１５２、公開鍵認証部１５３、秘密鍵記憶部１５４、証明書記憶部１５５、公開鍵記憶部１５６、証明書記憶部１５７、および証明書失効リスト記憶部１５８から構成されている。

通信部１５１は、インターネット２１を介して、親機１２－１、親機１２－２、およびバリュー発行装置１４から送信された信号を受信するとともに、親機１２－１、親機１２－２、およびバリュー発行装置１４に信号を送信する。通信部１５１は、データバス１５２を介して、公開鍵認証部１５３と接続されている。

公開鍵認証部１５３は、公開鍵記憶部１５６に記憶された公開鍵と、一般公開用証明書記憶部１５７に記憶された一般公開用証明書を公開したり、電子証明書を発行する。また、公開鍵認証部１５３は、電子証明書が有効であるかどうかを判定する。

秘密鍵記憶部１５４には、秘密鍵４２が記憶される。証明書記憶部１５５には、認証装置１３の電子証明書が記憶される。公開鍵記憶部１５６には、親機１２－１の秘密鍵３５に対応する公開鍵３９、親機１２－２の秘密鍵３８に対応する公開鍵４０、およびバリュー発行装置１４の秘密鍵４３に対応する公開鍵４１が記憶される。

一般公開用証明書記憶部１５７には、公開鍵認証部１５３が発行した一般公開用の電子証明書が記憶され、この電子証明書が親機１２やバリュー発行装置１４に提供される。証明書失効リスト記憶部１５８には、失効した電子証明書を示す証明書失効リストが記憶される。即ち、一般公開用証明書記憶部１５７に記憶された電子証明書が何らかの理由により失効したとき、その電子証明書が、その証明書失効リストにエントリされる。

図１８は、図１７の認証装置１３が電子証明書の判定を行う処理を説明するフローチャートである。この処理は、親機１２などから電子証明書の有効性の判定を要求する信号を受信したとき開始する。

ステップＳ１８１において、公開鍵認証部１５３は、証明書失効リスト記憶部１５８から、失効した電子証明書を示す証明書失効リストを読み出し、ステップＳ１８２に進む。ステップＳ１８２において、公開鍵認証部１５３は、親機１２から受信した電子証明書の判定を要求する信号に基づいて、判定の対象となる電子証明書が失効しているかどうかを判定する。即ち、公開鍵認証部１５３は、ステップＳ１８１で読み出された証明書失効リストに、判定の対象となる電子証明書があるかどうかを判定する。

ステップＳ１８２において、公開鍵認証部１５３は、判定の対象となる電子証明書が失効していると判定した場合、ステップＳ１８３に進み、データバス１５２を介して通信部１５１から、親機１２に電子証明書の無効通知を送信して処理を終了する。

ステップＳ１８２において、公開鍵認証部１５３は、判定の対象となる電子証明書が失効していないと判定した場合、ステップＳ１８４に進み、データバス１５２を介して通信部１５１から、親機１２に電子証明書の有効通知を送信して処理を終了する。

図１９は、図１の通信システム１の全体の処理を説明するフローチャートである。即ち、図１９のフローチャートは、移動端末装置１１－１と移動端末装置１１－２が親機１２－１とのみ直接無線通信することができる場合に、その親機１２－１に接続されたリソース機器１５－１を利用するときの通信システム全体の処理を示している。

なお、図１９では、移動端末装置１１－１、移動端末装置１１－２、親機１２－１、親機１２－１、認証装置１３、およびバリュー発行装置１４は、それぞれが通信する間で改ざんが行われず、正当な関係であるとする。

また、図１９では、まず最初に、移動端末装置１１－１がその本親機である親機１２－１にリソースを要求し、その後、移動端末装置１１－２が、無線通信できるが本親機でない親機１２－１にリソースを要求するものとする。

ステップＳ２３１において、移動端末装置１１－１は、その本親機である親機１２－１と双方向認証するために、共通秘密鍵３１を暗号化して、親機１２－１に送信する。

ステップＳ２５１において、親機１２－１は、移動端末装置１１－１から暗号化された共通秘密鍵３１を受信する。ステップＳ２５２において、親機１２－１は、共通秘密鍵３３を暗号化し、移動端末装置１１－１に送信する。

ステップＳ２３２において、移動端末装置１１－１は、親機１２－１から暗号化された共通秘密鍵３３を受信する。ステップＳ２３３において、移動端末装置１１－１は、その暗号化された共通秘密鍵３３を復号し、復号した共通秘密鍵３３を暗号化して、暗号化した共通秘密鍵３３を親機１２－１に送信する。

ステップＳ２５３において、親機１２－１は、暗号化された共通秘密鍵３３を、移動端末装置１１－１から受信する。ステップＳ２５４において、親機１２－１は、暗号化された共通秘密鍵３３を復号する。親機１２－１は、復号した共通秘密鍵３３から、親機１２－１と移動端末装置１１－１の関係が正当であるかどうかを判定する。この例では、親機１２－１と移動端末装置１１－１は正当な関係であるので、親機１２－１は、ステップＳ２５１で移動端末装置１１－１から受信した暗号化された共通秘密鍵３１を復号し、その復号した共通秘密鍵３１を暗号化して、移動端末装置１１－１に送信する。

ステップＳ２３４において、移動端末装置１１－１は、親機１２－１から暗号化された共通秘密鍵３１を受信し、その暗号化された共通秘密鍵３１を復号する。移動端末装置１１－１は、復号した共通秘密鍵３１から、親機１２－１と移動端末装置１１－１の関係が正当であるかどうかを判定する。この例では、親機１２－１と移動端末装置１１－１の関係は正当であるので、双方向認証を完了し、ス

テップＳ２３５において、移動端末装置１１－１は、リソースを要求する信号を親機１２－１に送信する。

即ち、移動端末装置１１－１は、その本親機である親機１２－１と双方向認証することにより、移動端末装置１１－１を使用するユーザが正しいユーザであることを、通信システム１のユーザに保証する。

ステップＳ２５５において、親機１２－１は、移動端末装置１１－１からリソースを要求する信号を受信する。ステップＳ２５６において、親機１２－１は、リソースを要求する信号に基づいて、要求対象となるリソース機器１５－１にリソースを要求する信号を送信する。

ステップＳ２９１において、リソース機器１５－１は、親機１２－１からリソースを要求する信号を受信する。ステップＳ２９２において、リソース機器１５－１は、リソースを要求する信号に基づいて、要求対象となるリソースを親機１２－１を介して、移動端末装置１１－１に送信する。

ステップＳ２３６において、移動端末装置１１－１は、リソース機器１５－１から親機１２－１を介して、リソースを受信し、これにより、リソース機器１５－１を利用することが可能な状態となる。

一方、移動端末装置１１－２は、ステップＳ２０１において、リソース情報を取得するために、その本親機でない親機１２－１にデバイス探索を要求する信号を送信する。

ステップＳ２５７において、親機１２－１は、移動端末装置１１－２からデバイス探索を要求する信号を受信し、デバイス探索要求を許可するかどうかを判定する。図１９では、ステップＳ２５８において、親機１２－１は、デバイス探索を許可し、デバイス探索を許可する信号を、移動端末装置１１－２に送信する。

ステップＳ２０２において、移動端末装置１１－２は、親機１２－１からデバイス探索を許可する信号を受信する。ステップＳ２０３において、移動端末装置１１－２は、親機１２－１が取得できるリソースの情報（親機１２－１が、移動

端末装置１１－２に提供することができるリソースの情報）を要求する信号を、親機１２－１に送信する。

ステップＳ２５９において、親機１２－１は、移動端末装置１１－２からリソースの情報を要求する信号を受信する。ステップＳ２６０において、親機１２－１は、リソース情報を移動端末装置１１－２に送信する。

ステップＳ２０４において、移動端末装置１１－２は、親機１２－１からリソース情報を受信する。ステップＳ２０５において、移動端末装置１１－２は、親機１２－２と双方向認証をするため、共通秘密鍵３２を暗号化し、その暗号化した共通秘密鍵３２を親機１２－２に送信する。

ステップＳ３１１において、親機１２－２は、移動端末装置１１－２から、暗号化された共通秘密鍵３２を受信する。ステップＳ３１２において、親機１２－２は、共通秘密鍵３６を暗号化し、暗号化した共通秘密鍵３６を移動端末装置１１-２に送信する。

ステップＳ２０６において、移動端末装置１１-２は、親機１２-２から暗号化した共通秘密鍵３６を受信し、暗号化した共通秘密鍵３６を復号する。移動端末装置１１－２は、復号した共通秘密鍵３６から、移動端末装置１１－２と親機１２-２の関係が正当であるかどうかを判定する。この例の場合、移動端末装置１１－２と親機１２－２の関係は正当であるので、ステップＳ２０７において、移動端末装置１１－２は、復号した共通秘密鍵３６を暗号化し、暗号化した共通秘密鍵３６を親機１２-２に送信する。

ステップＳ３１３において、親機１２－２は、移動端末装置１１－２から暗号化した共通秘密鍵３６を受信し、その暗号化した共通秘密鍵３６を復号する。親機１２－２は、復号した共通秘密鍵３６から、親機１２－２と移動端末装置１１-２の関係は正当であるかどうかを判定する。この例の場合、親機１２－２と移動端末装置１１－２の関係は正当であるので、ステップＳ３１４において、親機１２－２は、ステップＳ３１１で移動端末装置１１－２から受信した暗号化さ

れた共通秘密鍵３２を復号し、復号した共通秘密鍵３２を暗号化する。親機１２－２は、その暗号化した共通秘密鍵３２を移動端末装置１１－２に送信する。

ステップＳ２０８において、移動端末装置１１－２は、親機１２－２から暗号化された共通秘密鍵３２を受信し、その暗号化された共通秘密鍵３２を復号する。移動端末装置１１－２は、復号した共通秘密鍵３２から、移動端末装置１１－２と親機１２－２の関係が正当であるかどうかを判定する。この例では、移動端末装置１１－２と親機１２－２の関係が正当であるので、双方向認証を完了し、ステップＳ２０９において、移動端末装置１１－２は、リソースを要求する信号を親機１２－２に送信する。

ステップＳ３１５において、親機１２－２は、移動端末装置１１－２から、リソースを要求する信号を受信する。ステップＳ３１６において、親機１２－２は、親機１２－１にリソース情報の識別子と利用方法を明記した利用権発行要求と電子証明書を、親機１２－１に送信する。

ステップＳ２６１において、親機１２－１は、親機１２－２から利用権発行要求と電子証明書を受信する。ステップＳ２６２において、親機１２－１は、その電子証明書が有効であるかどうかの判定要求を認証装置１３に送信する。

ステップＳ３６１において、認証装置１３は、親機１２－１から電子証明書の判定要求を受信し、その電子証明書が有効であるかどうかを判定する。なお、ここでは、電子証明書は有効であるものとし、ステップＳ３６２において、認証装置１３は、親機１２－１に対象の電子証明書が有効であることを示す信号を送信する。

ステップＳ２６３において、親機１２－１は、認証装置１３から電子証明書が有効であることを示す信号を受信する。ステップＳ２６４において、親機１２－１は、リソースの利用を許可するための対価を記載したリソース利用条件文と電子証明書を、親機１２－２に送信する。

ステップＳ３１７において、親機１２－２は、親機１２－１からリソース利用条件文と電子証明書を受信する。ステップＳ３１８において、親機１２－２は、バリュー発行装置１４にバリュー移動要求を送信する。

ステップＳ３４１において、バリュー発行装置１４は、親機１２－２からバリュー移動要求を受信する。ステップＳ３４２において、バリュー発行装置１４は、親機１２－２と双方向認証するため、共通秘密鍵４４を暗号化して、暗号化した共通秘密鍵４４を親機１２－２に送信する。

ステップＳ３２０において、親機１２－２は、バリュー発行装置１４から、暗号化された共通秘密鍵４４を受信し、その暗号化された共通秘密鍵４４を復号する。親機１２－２は、復号した共通秘密鍵４４から、親機１２－２とバリュー発行装置１４の関係が正当であるかどうかを判定する。この例の場合、親機１２－２とバリュー発行装置１４の関係は正当であるので、ステップＳ３２０において、親機１２－２は、共通秘密鍵３７を暗号化し、暗号化した共通秘密鍵３７をバリュー発行装置１４に送信する。

ステップＳ３４３において、バリュー発行装置１４は、親機１２－２から暗号化された共通秘密鍵３７を受信し、その暗号化された共通秘密鍵３７を復号する。バリュー発行装置１４は、復号した共通秘密鍵３７から、バリュー発行装置１４と親機１２－２の関係が正当であるかどうかを判定する。この例の場合、バリュー発行装置１４と親機１２－２の関係は正当であるので、ステップＳ３４４において、バリュー発行装置１４は、ステップＳ３４１で受信したバリュー移動要求に応じてバリューを移動し、即ち、ここでは、親機１２－１のユーザから親機１２－１のユーザにバリューを移動し、バリューが移動されたことを示す振込み通知と電子証明書を、親機１２－１に送信する。

ステップＳ２６５において、親機１２－１は、バリュー発行装置１４から、振込み通知書と電子証明書を受信する。ステップＳ２６６において、親機１２－１は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置１３に送信する。

ステップＳ３６３において、認証装置１３は、親機１２－１から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機１２－２の電子証明書は有効であるので、ステップＳ３６４において、認証装置１３は、親機１２－１に対象の電子証明書が有効であることを示す信号を送信する。

ステップＳ２６７において、親機１２－１は、認証装置１３から電子証明書が有効であることを示す信号を受信する。ステップＳ２６８において、親機１２－１は、リソースを利用する権利を記載した権利文を発行し、その権利文と電子証明書を親機１２－２に送信する。

ステップＳ３２１において、親機１２－２は、親機１２－１から送信されてくる権利文と電子証明書を受信する。ステップＳ３２２において、親機１２－２は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置１３に送信する。

ステップＳ３６５において、認証装置１３は、親機１２－２から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機１２－１の電子証明書は有効であるので、ステップＳ３６６において、認証装置１３は、親機１２－２に対象の電子証明書が有効であることを示す信号を送信する。

ステップＳ３２３において、親機１２－２は、認証装置１３から電子証明書が有効であることを示す信号を受信する。ステップＳ３２４において、親機１２－２は、ステップＳ３２１で、親機１２－１から受信した権利文を、移動端末装置１１－２に送信する。

ステップＳ２１０において、移動端末装置１１－２は、親機１２－１から権利文を受信する。ステップＳ２１１において、移動端末装置１１－２は、その権利文とリソースを要求する信号を、親機１２－１に送信する。

ステップＳ２６９において、親機１２－１は、移動端末装置１１－２から、権利文とリソースを要求する信号を受信する。ステップＳ２７０において、親機１２－１は、リソース機器１５－１にリソースを要求する信号を送信する。

ステップＳ２９３において、リソース機器１５－１は、親機１２－１からリソースを要求する信号を受信する。ステップＳ２９４において、リソース機器１５－１は、親機１２－１から要求されたリソースを親機１２－１を介して、移動端末装置１１－２に送信する。

ステップＳ２１２において、リソース機器１５－１から、リソースを受信する。

以上により、移動端末装置１１－２は、親機１２－１から権利文を取得することにより、親機１２－１に接続されたリソース機器１５－１を利用できる環境を得ることができる。

以上のように、通信システム１では、バリュー発行装置１４は、バリューの管理をする親機１２に対して共通秘密鍵４４と同一の秘密鍵３４や３７を送信し、親機１２の非接触ＩＣカード１２１に記憶させる。親機１２は、個人情報を格納するユーザに、親機１２と通信可能にするための共通秘密鍵を格納した非接触ＩＣカード７１を発行する。これにより、ユーザは、非接触ＩＣカード７１の情報を移動端末装置１１に読み込ませるだけで、本親機である親機１２と通信をし、バリューの移動をすることができる。そして、ユーザは、上述した一連の処理を、例えば、非接触ＩＣカード７１を移動端末装置１１に、ワンタッチすることで行わせることができ、この場合、利便性の高い付加価値を提供することができる。

さらに、認証情報やそれに伴うユーザの個人情報を管理する本親機となる親機１２を、例えばユーザ宅のホームサーバという形で、移動端末装置１１とは別に設けたので、ユーザと移動端末装置１１とは依存関係がなく、リソースの利用時にのみユーザの認証を行えば済む。また、ユーザは、個人情報をバリュー発行装置に管理させることなく、自らの所有する親機１２に格納し、バリューの決済情報だけを親機１２とバリュー発行装置１４との間でやりとりするだけで済む。さらに、ユーザが移動する場合においても、ユーザは、移動した空間にある機器

（リソース）を、匿名のままユーザの嗜好に合わせた操作性で操作することができる。

また、図１の通信システム１によれば、ユーザが、移動した空間にある移動端末装置１１－２を操作することにより、そのユーザが個人情報を管理する親機（本親機）１２－２が、バリュー発行装置１４の仲介の下、他人の親機１２－１に電子バリューを支払って、その親機１２－１のリソースの利用権を入手し、その利用権を、移動端末装置１１－２が受け取って、親機１２－１に提示することで移動端末装置１１－２のユーザは、他人の親機１２－１のリソースを、匿名のまま利用することができる。即ち、バリュー発行装置１４は、移動端末装置１１－２のユーザの親機１２－２から他人の親機１２－１に対しての電子バリューの振込みを仲介するだけであり、ユーザの個人情報の管理は、親機１２で行われる。従って、電子バリューの決済の場と、個人情報の管理の場とが完全に分離されているということができる。なお、移動端末装置１１－２からバリュー発行装置１４にアクセスし、電子バリューを、リソースを利用しようとする親機１２－１に振込み、移動端末装置１１－２から親機１２－１のリソースを利用することも可能である。但し、この場合、親機１２－１に対する、移動端末装置１１－２のユーザの匿名性は確保されるが、移動端末装置１１－２のユーザの個人情報の管理は、移動端末装置１１－２がアクセスするバリュー発行装置１４で行われることになる。

さらに、移動端末装置１１－２は、リソースを利用する親機１２－１を介して、本親機である親機１２－２にアクセスして、そのリソースの利用権を取得するので、利用したいリソースに近い位置で、その利用権を得ることができる。

ここで、移動端末装置１１としては、例えば、PDA(Personal Digital Assistant)や、携帯用コンピュータ、携帯電話機、腕時計、ディジタルスチルカメラ、デジタルビデオカメラなどの携帯性に優れた装置を採用することが可能である。

また、出先のユーザが移動端末装置１１から利用するリソースとしては、例えば、「装置」や、「情報」、「情報に対するライセンス」などがある。

リソースとしての「装置」には、例えば、無線アクセスポイントや、テレビジョン受像機、電話機などが含まれる。リソースとして「装置」を利用するケースとしては、例えば、出先のユーザが、移動端末装置１１から、他人の無線アクセスポイントを利用してインターネットに接続する場合がある。

また、リソースとしての「情報」には、いわゆるホームサーバやチャンネルサーバなどで構成される親機１２－１が管理するコンテンツその他の情報などが含まれる。リソースとして「情報」を利用するケースとしては、例えば、出先のユーザが、親機１２－１としてのチャンネルサーバに蓄えられたコンテンツを視聴する場合がある。

さらに、リソースとしての「情報に対するライセンス」には、情報が暗号化されている場合に、その暗号化を解くための鍵などが含まれる。リソースとして「情報に対するライセンス」を利用するケースとしては、例えば、携帯端末装置１１に、ネットワーク経由でダウンロードした、暗号化されたコンテンツを視聴する場合に、そのコンテンツを視聴するためのライセンスとしての暗号鍵を取得するときなどがある。

なお、上述した一連の処理では、移動端末装置１１－１と移動端末装置１１－２のユーザは異なっていたが、同一ユーザの親機や移動端末装置間でも同様に電子バリューの移動をすることができる。

上述した実施の形態に関し、具体例を挙げてさらに説明を加える。

図２０は、ユーザＢがユーザＡの家で、ユーザＡのＰＣ（パーソナルコンピュータ）を借り、その対価を支払う例を説明するための図であり、そのような場合におけるシステムの構成例を示している。移動端末装置２０１―１は、ユーザＡが所持する装置であり、移動端末装置２０１―２は、ユーザＢが所持する装置である。移動端末装置２０１－１，２０１―２は、それぞれ携帯電話や、携帯可能なＣＤプレーヤなどである。

移動端末装置２０１―１には、ユーザＡのホームサーバ２０２－１のアドレスが登録され、移動端末装置２０１―２には、ユーザＢのホームサーバ２０２－２のアドレスが登録されている。

ユーザＡが管理するホームサーバ２０２―１は、同じくユーザＡが管理しているＰＣ２０３やＴＶ（テレビジョン受像機）２０４を管理する。このＰＣ２０３やＴＶ２０４は、家庭内ネットワークを介してホームサーバ２０２―１と接続されているリソースである。また、ホームサーバ２０２―１は、ユーザＡの個人情報も保管している。

同様に、ユーザＢが管理するホームサーバ２０２―２は、ユーザＢが管理するリソースを管理すると共に、ユーザＢの個人情報も保管する。ホームサーバ２０２－１やホームサーバ２０２－２は、それぞれ無線により直接的に、または、アクセスポイント（図２０においては不図示）を介して他のホームサーバと通信することができるように構成されている。

また、携帯端末装置２０１－１，２０１－２は、接続したホームサーバ２０２―１，２０２－２を介し、そしてインターネット２０５を経由し、他のホームサーバなどと通信することができるように構成されている。

インターネット２０５には、認証装置２０６も接続されている。認証装置２０６は、ＰＫＩ処理のための証明書を発行する機関が管理する装置であり、証明書の管理を行うための装置である。インターネット２０５には、バリュー発行装置２０７も接続されている。バリュー発行装置２０７は、各ユーザのバリューの交換を仲介する装置（対価の支払いに係わる処理を実行する装置）である。

ここで、図２０に示したシステムと図１に示したシステムとの対応関係を記載しておく。移動端末装置２０１―１は、移動端末装置１１－１であり、移動端末装置２０１－２は、移動端末装置１１－２である。ホームサーバ２０２－１は、親機１２－１であり、ホームサーバ２０２－２は、親機１２－２である。ＰＣ２０３は、リソース機器１６－２であり、ＴＶ２０４は、リソース機器１５－２である。

インターネット２０５は、インターネット２１であり、認証装置２０６は、認証装置１３である。バリュー発行装置２０７は、バリュー発行装置１４である。このように、図２０は、図１と対応関係があり、図１およびそれ以降の図を参照して説明した事項は、図２０に示したシステムに関する事項として適用できるため、既に説明した部分については、適宜説明を省略する。

次に、図２１のフローチャートを参照し、ユーザＢが移動端末装置２０１－２を保持している状態でユーザＡ宅に行き、ユーザＡ宅に設置され、ユーザＡにより管理されているＰＣ２０３を使用するときに、図２０に示したシステムで行われる処理について説明する。なお、以下の説明においては、認証局（認証装置２０６）でＰＫＩにより行われる、各ユーザのアクセスの信頼性を確認する手順については、既に説明した事項と重なるため省略する。

まず、移動端末装置の初期化に係わる処理が実行される。移動端末装置の初期化に係わる処理は、ここでは、移動端末装置２０１―２とホームサーバ２０２－２との間で行われる。まずステップＳ４０１において、ユーザＢが保持する移動端末装置２０１―２は、ホームサーバ２０２―２にアクセスする。

ステップＳ４７１において移動端末装置２０１―２からのアクセスを受けたホームサーバ２０２―２は、ステップＳ４７２において、自己が管理しているユーザＢの個人情報の一部を送信する。送信された個人情報は、ステップＳ４０２において、移動端末装置２０１―２に受信され、保持される。

移動端末装置２０１―２には、ホームサーバ２０２―２のアドレスが登録されているため、ホームサーバ２０２―２にアクセスすることが可能とされている。また、移動端末装置２０１―２は、ユーザＢが登録されており、ユーザＢしか使うことができないように構成されている。例えば、ユーザＢの指紋が登録されており、指紋認証が正常に行われない限り、移動端末装置２０１―２は起動されないように構成されている。

そして、指紋認証などが用いられた認証処理が正常に行われた後（この場合、ユーザＢであると確認がとれた後）、移動端末装置２０１―２は、使用可能な状

態とされる。使用可能な状態とされた後、ホームサーバ２０２―２とアクセス可能で有れば、上述したような処理が、移動端末装置２０１―２とホームサーバ２０２－２との間で実行される。

移動端末装置２０１―２は、ユーザＢの個人情報を保持した後の時点で、定期的にデバイス探索要求を発信している（ステップＳ４０３）。その定期的に発信されているデバイス探索要求を、ステップＳ４２１の処理として受信したホームサーバ２０２－１は、ステップＳ４２２において、自己のアドレス、デバイス探索要求を発信してきた端末（この場合、移動端末装置２０１－２）に一時的に与えるＩＤ、および、移動端末装置２０１－２がインターネット２０５を介して他の装置とデータの授受を行えるようにするために必要となる情報（例えば、デフォルトルータのアドレスなど）を、移動端末装置２０１－２に通知する。

このようなホームサーバ２０２－１からのデータは、ステップＳ４０４において、移動端末装置２０１－２に受信され、記憶される。ステップＳ４０５において、移動端末装置２０１－２は、ホームサーバ２０２－２に対してリソース要求を出す。移動端末装置２０１－２は、先程の処理で、ホームサーバ２０２－２のアドレスを取得し記憶しているため、ホームサーバ２０２－２と通信することができる状態とされている。なお、この通信の際、必要に応じ、ホームサーバ２０２－１から与えられたＩＤも用いられる。

ステップＳ４２３において、ホームサーバ２０２－１は、リソース要求を受信すると、ステップＳ４２４の処理として、自己の管理するリソースに関する情報を、移動端末装置２０１－２に対して通知する。リソース情報として、ホームサーバ２０２－１から移動端末装置２０１－２に対して通知される情報について説明する。

リソース情報は、リソースの名前、設置場所、現在使用中であるか否かを表す情報、使用する際に必要となる対価、移動端末装置から操作できる操作のリストなどを含む情報である。例えば、図２０を参照するに、ホームサーバ２０２－１には、ＰＣ２０３が接続されている。ＰＣ２０３に関するリソース情報としては、

ＰＣ２０３という名称であり、例えば、居間に設置され、現在使用中ではなく、対価として例えば１００円を必要とし、移動端末装置２０１－２から操作できる操作のリストを含む情報である。

同様のリソース情報が、ホームサーバ２０２－１に接続されているＴＶ２０４に関しても作成され、ＰＣ２０３のリソース情報と合わせて、移動端末装置２０１－２に対して通知される。

このようなリソース情報を、ステップＳ４０６の処理として受信した移動端末装置２０１－２は、そのリソース情報を記憶する。

このようにして、リソース情報を取得した移動端末装置２０１－２は、次に、リソースの選択に係わる処理を実行する。

まず前提として、移動端末装置２０１－２は、取得したリソース情報を基に、ユーザにリソースに関する情報を提示する。提示の仕方は、どのようなものでも良いが、例えば、移動端末装置２０１－２は、図２に示すような構成を有し、表示部６４を有していれば、その表示部６４を用いて提示が行われるように構成する。具体的には、まず表示部６４に、リソースの一覧（この場合、例えば、ＰＣ２０３とＴＶ２０４が列記されたものである）が表示される。その一覧を参照しユーザＢが、使用したいリソース（機器）を選択すると、その選択された機器に関する詳細な情報に、表示部６４の表示が切り換えられる。

このようにして、ホームサーバ２０２－１から詳細情報まで含まれるリソース情報が通知され、段階的にユーザに提示されるようにしても良い。

他のリソース情報の提示の仕方としては、リソース（例えば、ＰＣ２０３）と直接的に近接通信を行うことにより、そのリソースの詳細な情報が取得されるようにしても良い。例えば、まず、ステップＳ４０７において、移動端末装置２０１－２からＰＣ２０３に対して、近接通信によりリソース情報の要求が出される。

そのような要求をステップＳ４５１において受信したＰＣ２０３は、ステップＳ４５２において、自己の詳細な情報（例えば、使用するのに必要とされる金額など）を移動端末装置２０１－２に対して通知する。そのような通知を、ステッ

プＳ４０８において受信した移動端末装置２０１－２は、その受信した情報を、ユーザＢに対して提示する。

いずれの手順により、リソース情報が移動端末装置２０１－２に対して通知されるようにしても良いが、結果としてユーザＢは、リソース情報を参照し、使用したい機器を選択する。ここでは、ユーザＢは、ＰＣ２０３を使用したい機器として選択したとして説明を続ける。

ユーザＢが、使用したい機器としてＰＣ２０３を選択すると、移動端末装置２０１－２の表示部６４には、“１時間１００円で使用しますか？”といったようなメッセージが表示される。これは、ユーザＡが所有するＰＣ２０３を使用することにより、その対価を支払わなくてはならないといったようなことをユーザＢに認識させるためのものである。ユーザＢは、そのようなメッセージを確認し、対価を支払ってＰＣ２０３を使用する場合、所定の操作、例えば、表示部６４に表示された“ＹＥＳ”といったようなボタン（不図示）を操作する。

そのような操作が行われた場合、移動端末装置２０１－２は、ステップＳ４０９において、ホームサーバ２０２－２に対して、使用したいリソース（この場合、ＰＣ２０３）と、そのリソースを管理するホームサーバ（この場合、ホームサーバ２０２－１）のアドレスを通知する。このような通知を、ステップＳ４７３の処理として受信したホームサーバ２０２－２は、ステップＳ４７４において、ホームサーバ２０２－１に対して、当該リソースの使用を要求する旨と、使用条件（この場合、例えば、１時間使用するという条件）を通知する。

このような通知を、ステップＳ４２５の処理として受信したホームサーバ２０２－１は、ステップＳ４２６において、自己に登録された機器（リソース）情報から、通知された使用条件（この場合、１時間使用するという条件）を満たすために、ユーザＢが支払うべき対価（この場合、１時間×１００円＝１００円という計算がなされる）を算出し、その算出結果を、トランザクション番号と共に、ホームサーバ２０２－２に対して通知する。

ステップＳ４７５において、ホームサーバ２０２－１からの通知を受信したホームサーバ２０２－２は、ステップＳ４７６において、バリュー発行装置２０７に対して、トランザクション番号と共に、ホームサーバ２０２－１宛にバリューの振り込み要求を行う。バリュー発行装置２０７は、ステップＳ４９１において、ホームサーバ２０２－２からの通知を受信すると、ホームサーバ２０２－１との間で、バリューの振り込みの処理が実行される（ステップＳ４９２、ステップＳ４２７）。

またバリュー発行装置２０７は、ホームサーバ２０２－２との間で、バリューの減額処理を実行する（ステップＳ４９３、ステップＳ４７７）。このようにして、バリュー発行装置２０７は、ホームサーバ２０２－１に対してバリューの振り込みの処理を実行し、その振り込みされるバリューを、ホームサーバ２０２－２から減額するという処理を実行する。

バリューの振り込み、減額の処理がそれぞれ正常に行われると、バリュー発行装置２０７は、ステップＳ４９４において、ホームサーバ２０２－１に対して、トランザクションが正常に終了されたことを、トランザクション番号と共に通知する。

ホームサーバ２０２－１は、このような通知をバリュー発行装置２０７から、ステップＳ４２８において受信すると、ステップＳ４２９において、トランザクション番号から、使用を許可する（使用を要求されていた）機器、その使用条件、および、使用権を、ホームサーバ２０２－２に対して発行する。同様の情報を、ステップＳ４３０において、ホームサーバ２０２－１は、ＰＣ２０３に対しても発行する。

ステップ４７８において、ホームサーバ２０２－１により発行された使用権などを受信したホームサーバ２０２－２は、ステップＳ４７９において、移動端末装置２０１－２に対して、使用権を渡す。

ステップＳ４１０において、ホームサーバ２０２－２から使用権を受信した移動端末装置２０１－２は、ステップＳ４１１において、ＰＣ２０３に対して、使

用権を提示する。この提示は、ホームサーバ２０２－１を介して行われても良いし、直接的に近距離無線通信などが用いられて行われるようにしても良い。使用権を提示されたＰＣ２０７は、ステップＳ４５５において、まず、ホームサーバ２０２－１から渡された使用権と、移動端末装置２０１－２から提示された使用権が一致するか否かを判断する。

使用権が一致すると判断された場合、ステップＳ４５５において、ＰＣ２０７は、移動端末装置２０１－２に対してアクセス許可を通知する。なお、使用権が一致しないと判断された場合、ＰＣ２０７は、アクセス許可を通知しない（アクセス許可をしないということを通知するようにしても良い）。

ＰＣ２０７は、アクセス許可を通知することにより、また、移動端末装置２０１－２は、アクセス許可を通知されることにより、互いにデータの授受が行える状態とされる。すなわち、ＰＣ２０７は、移動端末装置２０１－２からの操作指示を受け入れる状態とされる。このように、移動端末装置２０１－２で、ＰＣ２０７を操作できる状態とされた場合、移動端末装置２０１－２の所有者であるユーザＢの嗜好が反映された形でＰＣ２０７を操作できるようにするための情報が、移動端末装置２０１－２からＰＣ２０７に対して通知される。

すなわち、ステップＳ４１３において、移動端末装置２０１－２は、ＰＣ２０７に対して、自己が管理しているユーザＢの嗜好情報を通知する。ＰＣ２０７は、そのような嗜好情報を受信すると、その嗜好情報に基づき、ユーザＢ用にカスタマイズされた環境を構築する。例えば、嗜好情報として、ユーザＢがいつも使用しているログイン画面に関する情報が通知された場合、その画面がログイン時にＰＣ２０７のディスプレイ（不図示）上に表示される。

このように、本発明を適用することにより、他のユーザが管理する装置を対価を支払って使用することが可能となる。

なお、本明細書において、フローチャートに記載された処理は、ステップとして記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列

的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。

産業上の利用可能性

本発明によれば、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作させることができる。また、そのとき発生する対価の支払いを自動的に行うことができる。さらに、利便性がよく、安全な通信をすることができる。

請求の範囲

1．　ユーザにより操作される端末と、

リソースを提供する第１の親機と、

前記ユーザの個人情報を記憶する第２の親機と、

電子バリューを管理するバリュー装置と

を備える情報処理システムにおいて、

前記端末は、

前記第１の親機が提供するリソースを要求する信号を、前記第２の親機に送信するリソース要求信号送信手段と、

前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する第１の利用権取得手段と

を有し、

前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用し、

前記第１の親機は、

前記リソースの提供に対する対価としての電子バリューが、前記第２の親機から前記第１の親機に振り込まれたことの振込み通知を、前記バリュー装置から受信する振込み通知受信手段と、

前記振込み通知に応じて、前記第２の親機に対して、前記利用権を発行する利用権発行手段と

を有し、

前記端末が、前記利用権を提示した場合に、自身が有するリソースの利用を許可し、

前記第２の親機は、

前記端末装置から送信されてくる、前記リソースを要求する信号に応じて、前記第１の親機への前記電子バリューの振込みを、前記バリュー装置に要求する電子バリュー振込み要求手段と、

前記電子バリューの振込みに応じて、前記第１の親機が発行する前記利用権を取得する第２の利用権取得手段と、

前記第２の利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段と

を有し、

前記バリュー装置は、

前記第２の親機からの要求に応じて、前記第１の親機に前記電子バリューを振り込む電子バリュー振込み手段と、

前記第１の親機への前記電子バリューの振込み通知を、前記第１の親機に送信する振込み通知送信手段と

を有する

ことを特徴とする情報処理システム。

２．　ユーザにより操作される情報処理装置において、

リソースを提供する第１の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信手段と、

前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する利用権取得手段と

を備え、

前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用する

ことを特徴とする情報処理装置。

３．　前記第２の親機との間で、前記ユーザが前記第２の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段を

さらに備えることを特徴とする請求の範囲第２項に記載の情報処理装置。

４．　前記リソース要求信号送信手段と前記利用権取得手段は、前記第１の親機を介して、前記第２の親機とやりとりする

ことを特徴とする請求の範囲第２項に記載の情報処理装置。

5． 前記リソース要求信号送信手段と前記利用権取得手段は、前記第２の親機との間で、データを暗号化してやりとりする

ことを特徴とする請求の範囲第２項に記載の情報処理装置。

6． 前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求の範囲第２項に記載の情報処理装置。

7． ユーザにより操作される情報処理装置の情報処理方法において、

リソースを提供する第１の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信ステップと、

前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用する

ことを特徴とする情報処理方法。

8． ユーザにより操作される情報処理装置に実行させるプログラムであって、

リソースを提供する第１の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信ステップと、

前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用する

ことを特徴とするプログラム。

9． ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置において、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段と

を備え、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理装置。

１０．　前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備える

ことを特徴とする請求の範囲第９項に記載の情報処理装置。

１１．　前記振込み通知が正当であることの認証を行う認証手段を

さらに備える

ことを特徴とする請求の範囲第９項に記載の情報処理装置。

１２．　前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求の範囲第９項に記載の情報処理装置。

１３．　ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置の情報処理方法において、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップと

を含み、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理方法。

１４．　ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置に実行させるプログラムであって、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップと

を含み、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とするプログラム。

１５．　ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置において、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段と、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段と、

前記利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段と

を備えることを特徴とする情報処理装置。

１６．　前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備える

ことを特徴とする請求の範囲第１５項に記載の情報処理装置。

１７．　前記端末との間で、前記ユーザが前記個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備える

ことを特徴とする請求の範囲第１５項に記載の情報処理装置。

１８．　前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求の範囲第１５項に記載の情報処理装置。

１９．　ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置の情報処理方法において、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とする情報処理方法。

２０．　ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置に実行させるプログラムにおいて、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とするプログラム。

２１．　電子バリューを管理する情報処理装置において、

ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込み手段と、

前記第２の親機から前記第１の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第１の親機に送信する振込み通知送信手段と

を備えることを特徴とする情報処理装置。

２２．　前記第１または第２の親機との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段を

さらに備えることを特徴とする請求の範囲第２１に記載の情報処理装置。

２３．　前記第１と第２の親機の電子バリューを記憶する記憶手段をさらに備え、

前記電子バリュー振込み手段は、前記記憶手段に記憶された電子バリューを書き換えることにより、前記第２の親機から前記第１の親機に対して、前記電子バリューを振り込む

ことを特徴とする請求の範囲第２１項に記載の情報処理装置。

２４．　前記電子バリュー振込み手段は、前記第２の親機から電子バリューを取得し、その電子バリューを前記第１の親機に送信することにより、

前記第２の親機から前記第１の親機に対して、前記電子バリューを振り込む

ことを特徴とする請求の範囲第２１項に記載の情報処理装置。

２５．　前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求の範囲第２１項に記載の情報処理装置。

２６．　前記電子バリューは、口座という形で管理され、

前記口座は、前記親機の証明書にある機器ＩＤ、または、その機器ＩＤに対応付けられたＩＤにより管理される

ことを特徴とする請求の範囲第２１項に記載の情報処理装置。

２７．　電子バリューを管理する情報処理装置の情報処理方法において、

ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込みステップと、

前記第２の親機から前記第１の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第１の親機に送信する振込み通知送信ステップとを含むことを特徴とする情報処理方法。

２８．　電子バリューを管理する情報処理装置に実行させるプログラムであって、

ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込みステップと、

前記第２の親機から前記第１の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第１の親機に送信する振込み通知送信ステップとを含むことを特徴とするプログラム。

図1

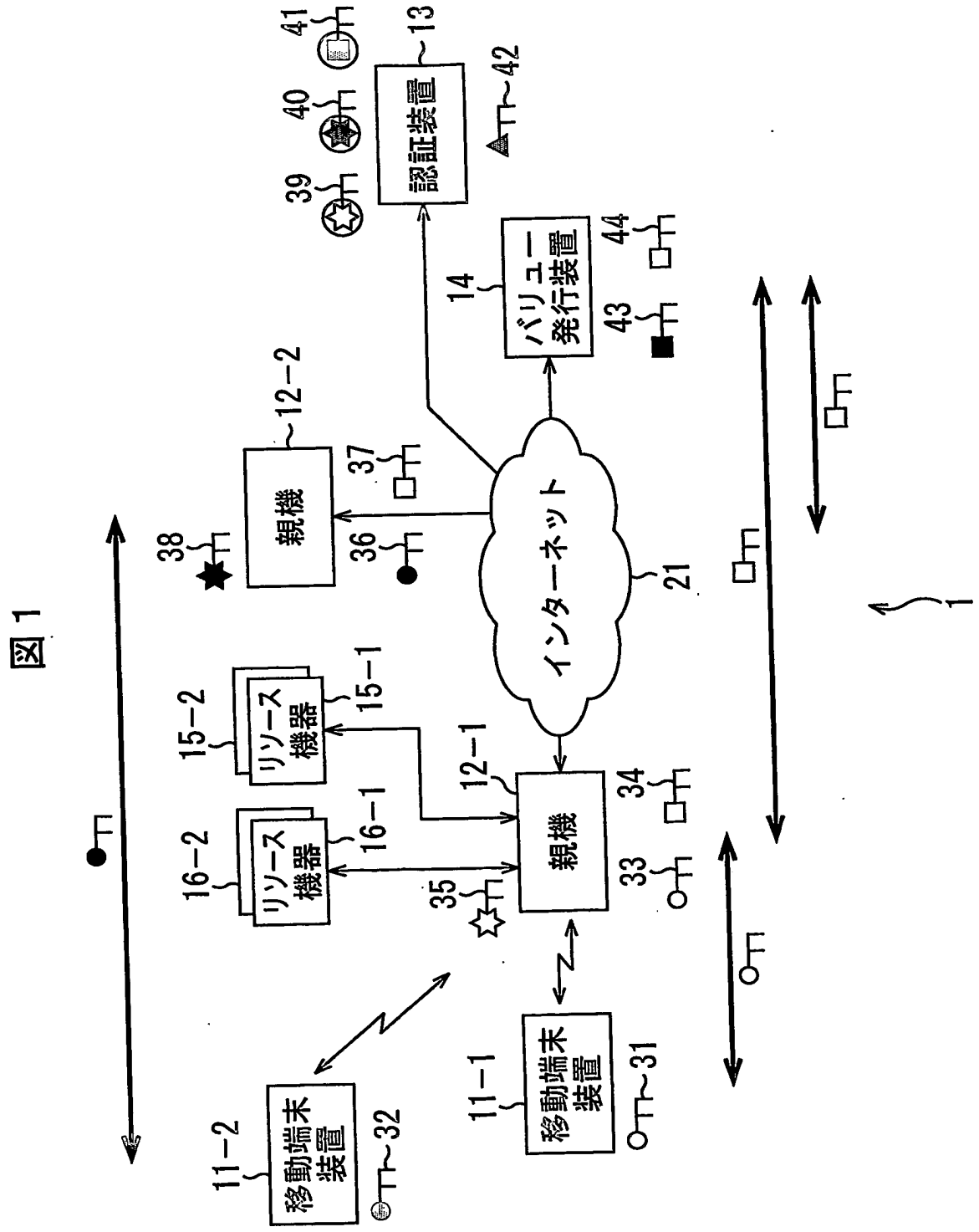

認証装置
13
41
42
40
39
バリュー発行装置
14
44
43
親機
12-2
37
38
36
インターネット
21
1
リソース機器
15-2
15-1
16-2
16-1
12-1
親機
34
35
33
移動端末装置
11-2
32
11-1
31

図2

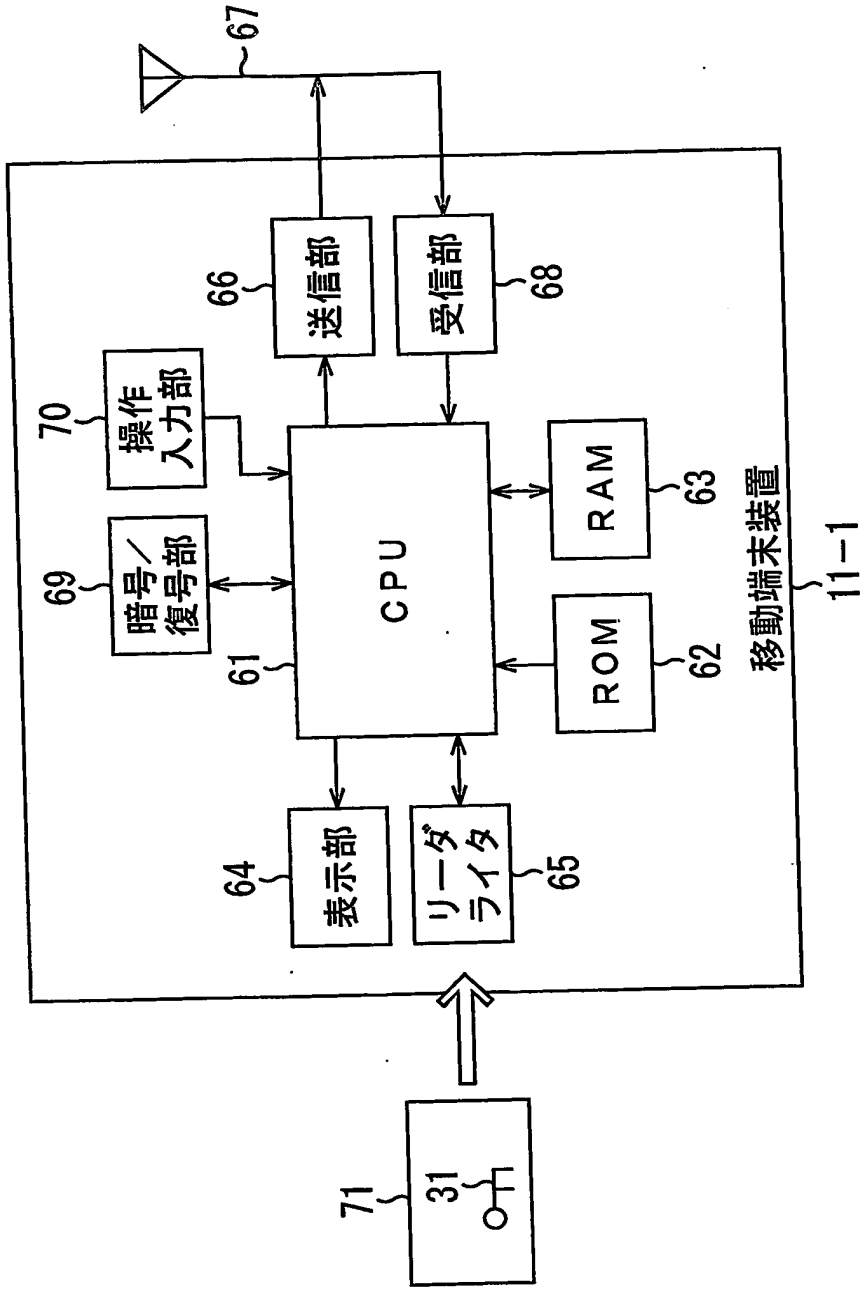

67
66
送信部
68
受信部
70
操作
入力部
69
暗号/
復号部
CPU
61
RAM
63
ROM
62
移動端末装置
11-1
64
表示部
リーダ
ライタ
65
71
31

図３

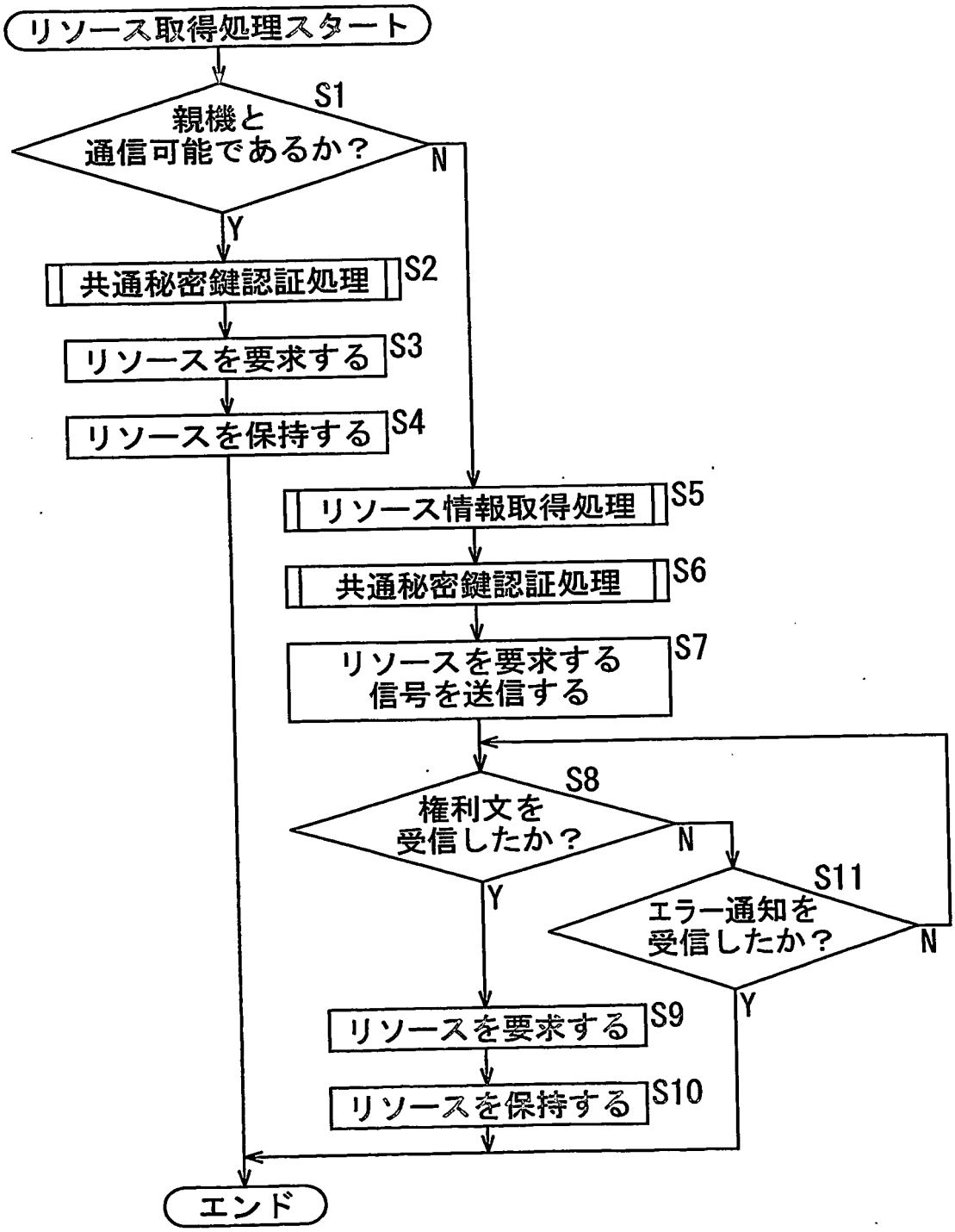

リソース取得処理スタート
S1
親機と
通信可能であるか？
N
Y
共通秘密鍵認証処理
S2
リソースを要求する
S3
リソースを保持する
S4
リソース情報取得処理
S5
共通秘密鍵認証処理
S6
リソースを要求する
信号を送信する
S7
S8
権利文を
受信したか？
N
Y
S11
エラー通知を
受信したか？
N
Y
リソースを要求する
S9
リソースを保持する
S10
エンド

図4

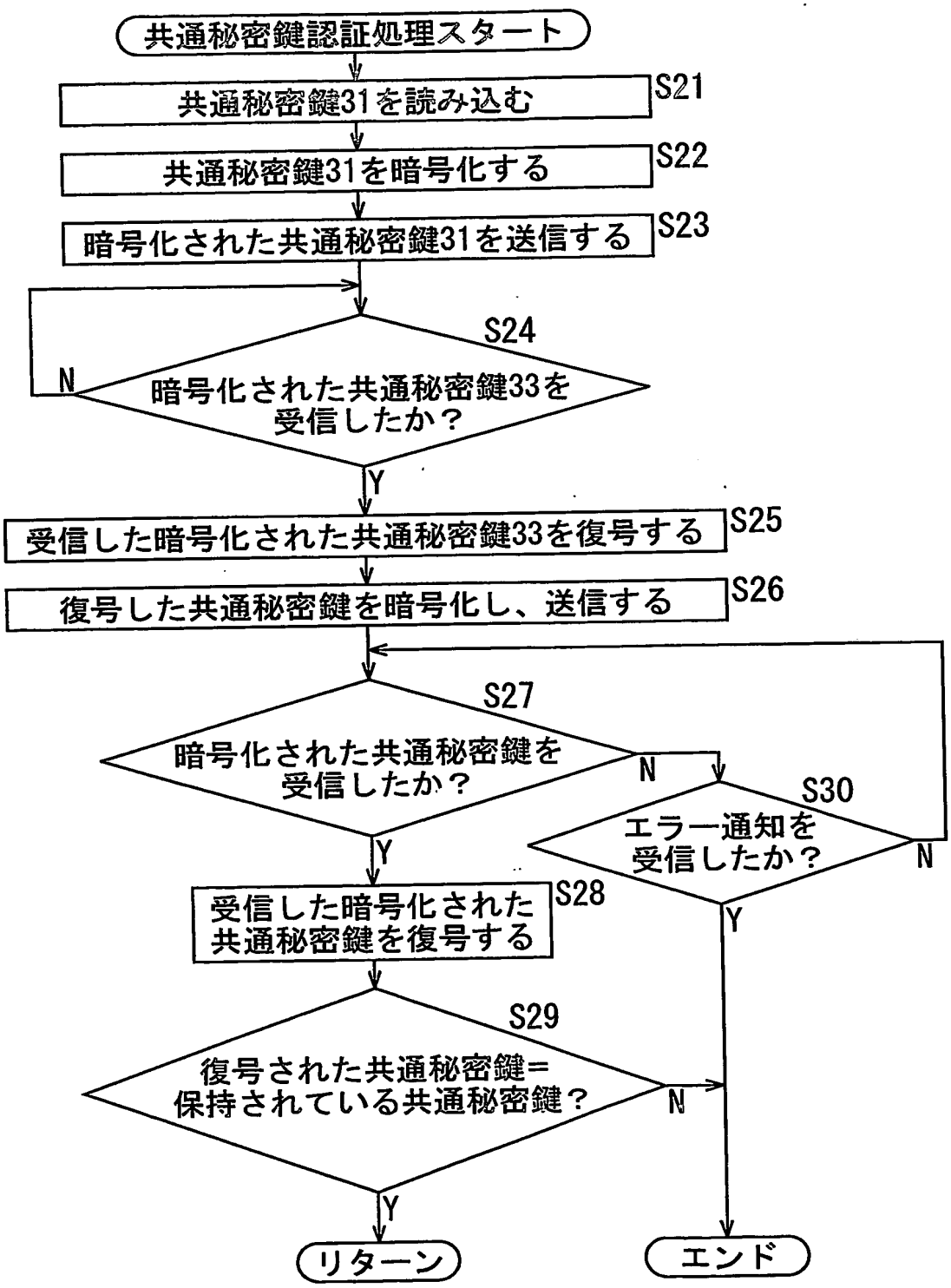

共通秘密鍵認証処理スタート
共通秘密鍵31を読み込む
S21
共通秘密鍵31を暗号化する
S22
暗号化された共通秘密鍵31を送信する
S23
S24
暗号化された共通秘密鍵33を受信したか？
N
Y
受信した暗号化された共通秘密鍵33を復号する
S25
復号した共通秘密鍵を暗号化し、送信する
S26
S27
暗号化された共通秘密鍵を受信したか？
N
Y
S30
エラー通知を受信したか？
N
Y
受信した暗号化された共通秘密鍵を復号する
S28
S29
復号された共通秘密鍵＝保持されている共通秘密鍵？
N
Y
リターン
エンド

図５

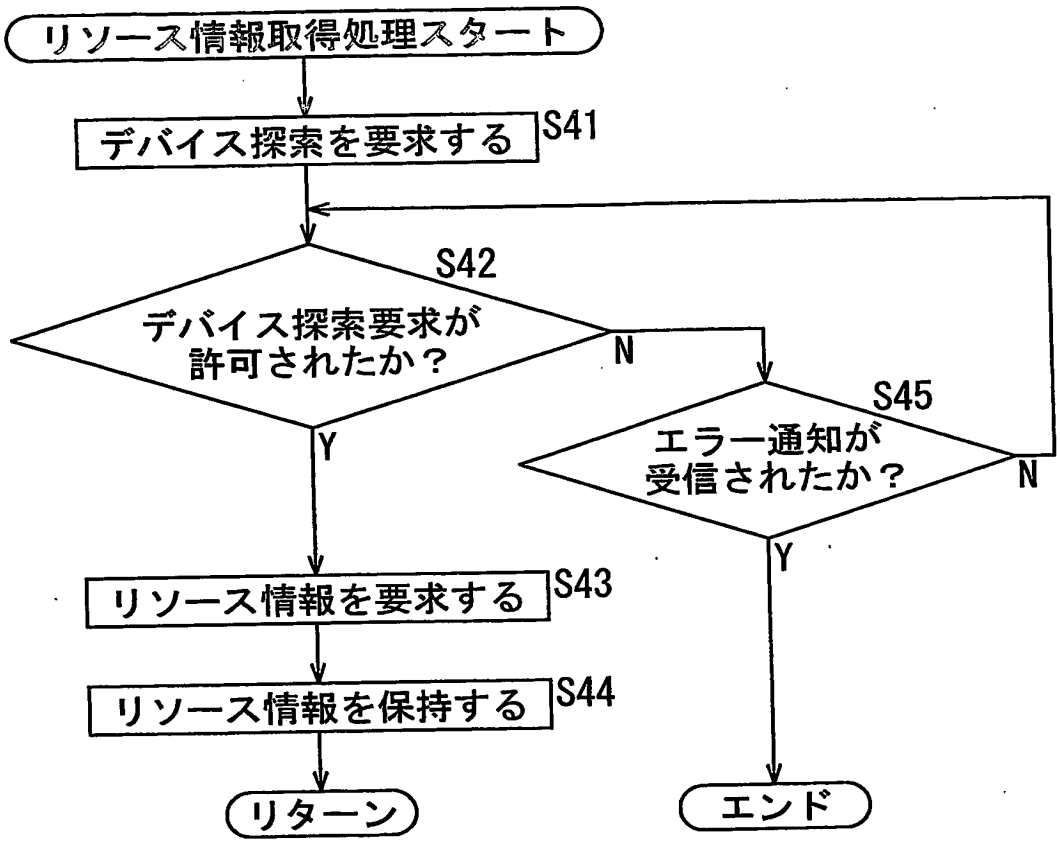

リソース情報取得処理スタート
デバイス探索を要求する
S41
S42
デバイス探索要求が
許可されたか？
N
Y
S45
エラー通知が
受信されたか？
N
Y
リソース情報を要求する
S43
リソース情報を保持する
S44
リターン
エンド

図6

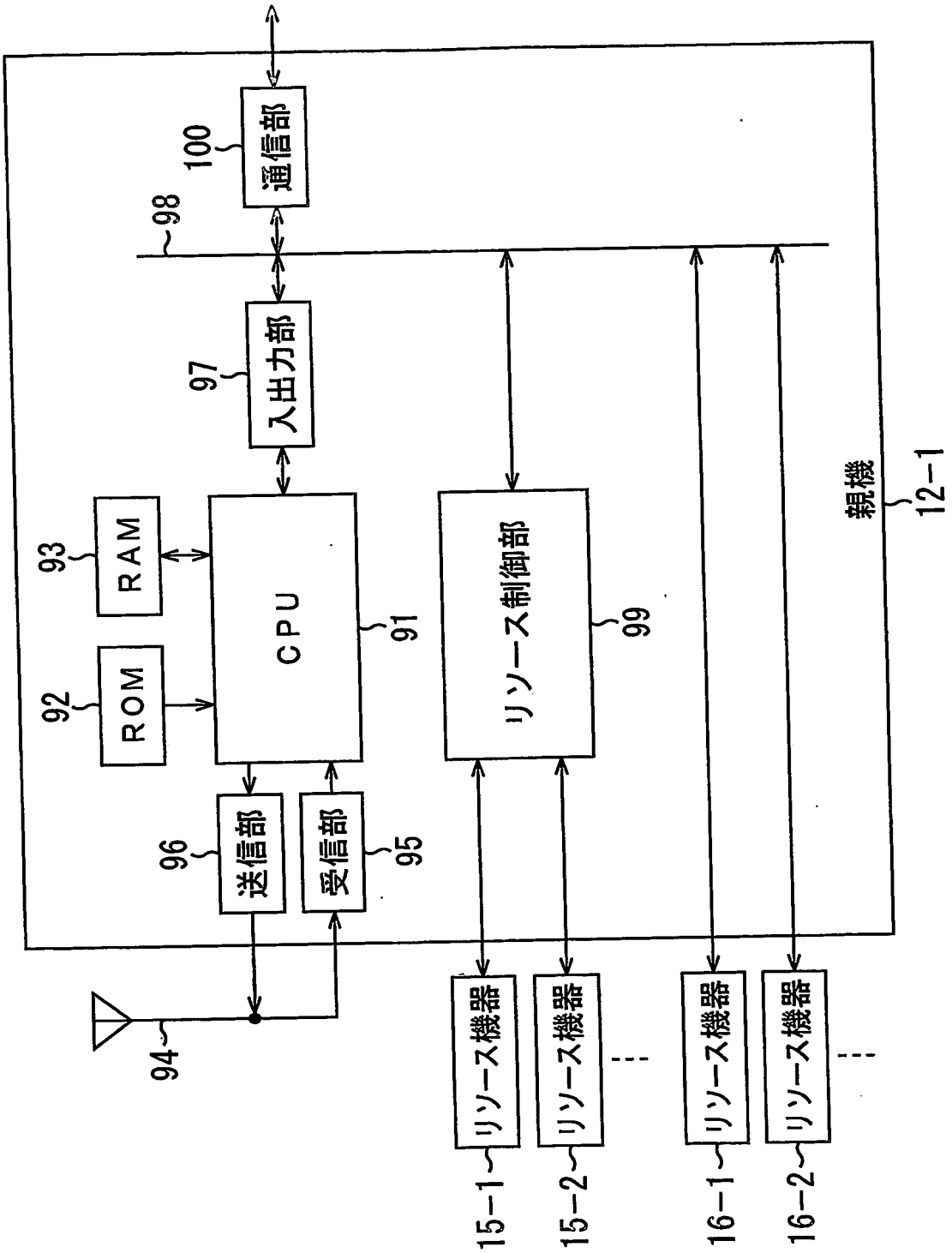

通信部
100
98
入出力部
97
RAM
93
ROM
92
CPU
91
リソース制御部
99
送信部
96
受信部
95
94
親機
12-1
リソース機器
15-1
リソース機器
15-2
リソース機器
16-1
リソース機器
16-2

図7

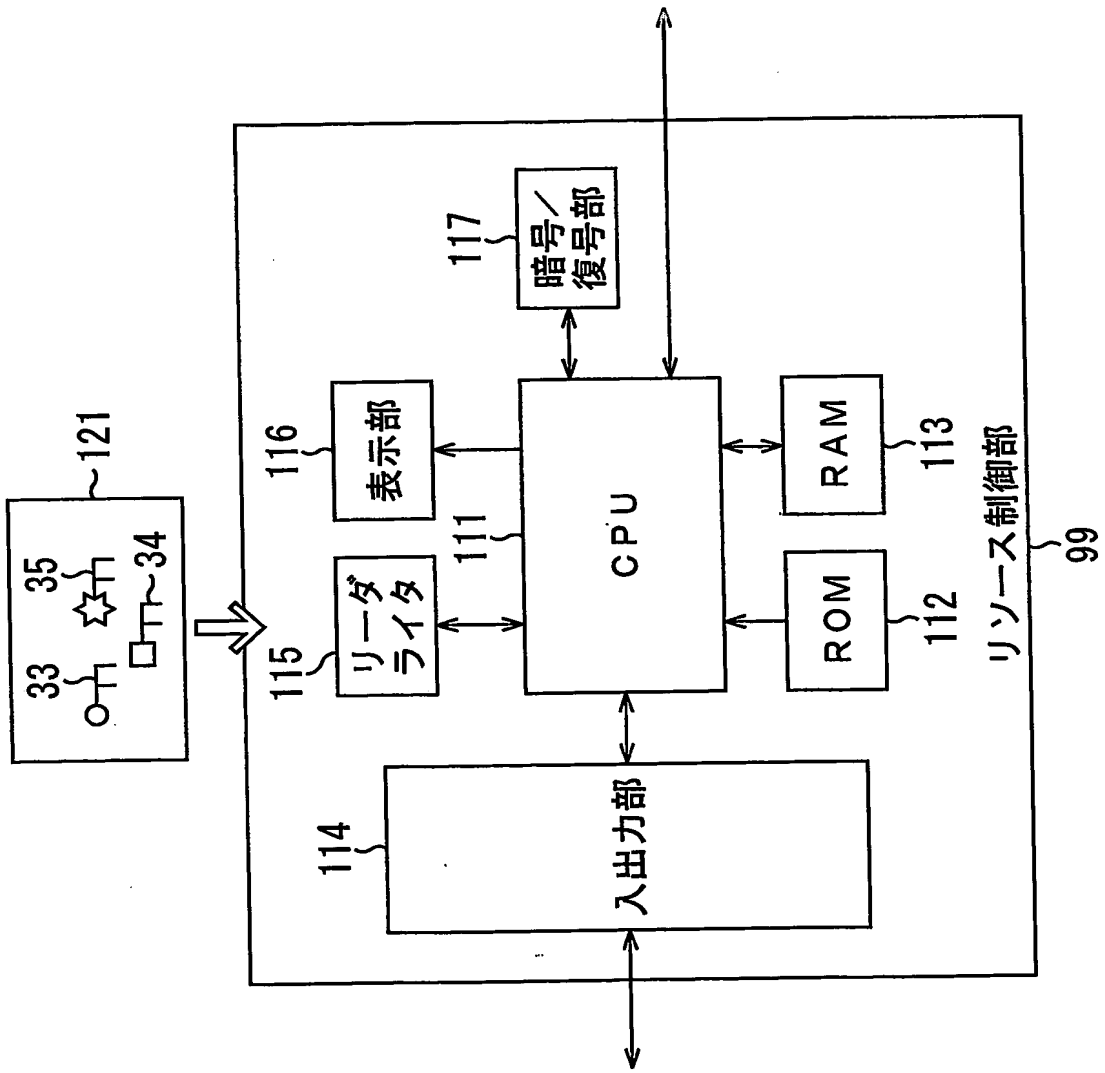

121
35
34
33
116
表示部
117
暗号／
復号部
111
CPU
RAM
113
115
リーダ
ライタ
ROM
112
リソース制御部
99
114
入出力部

図８

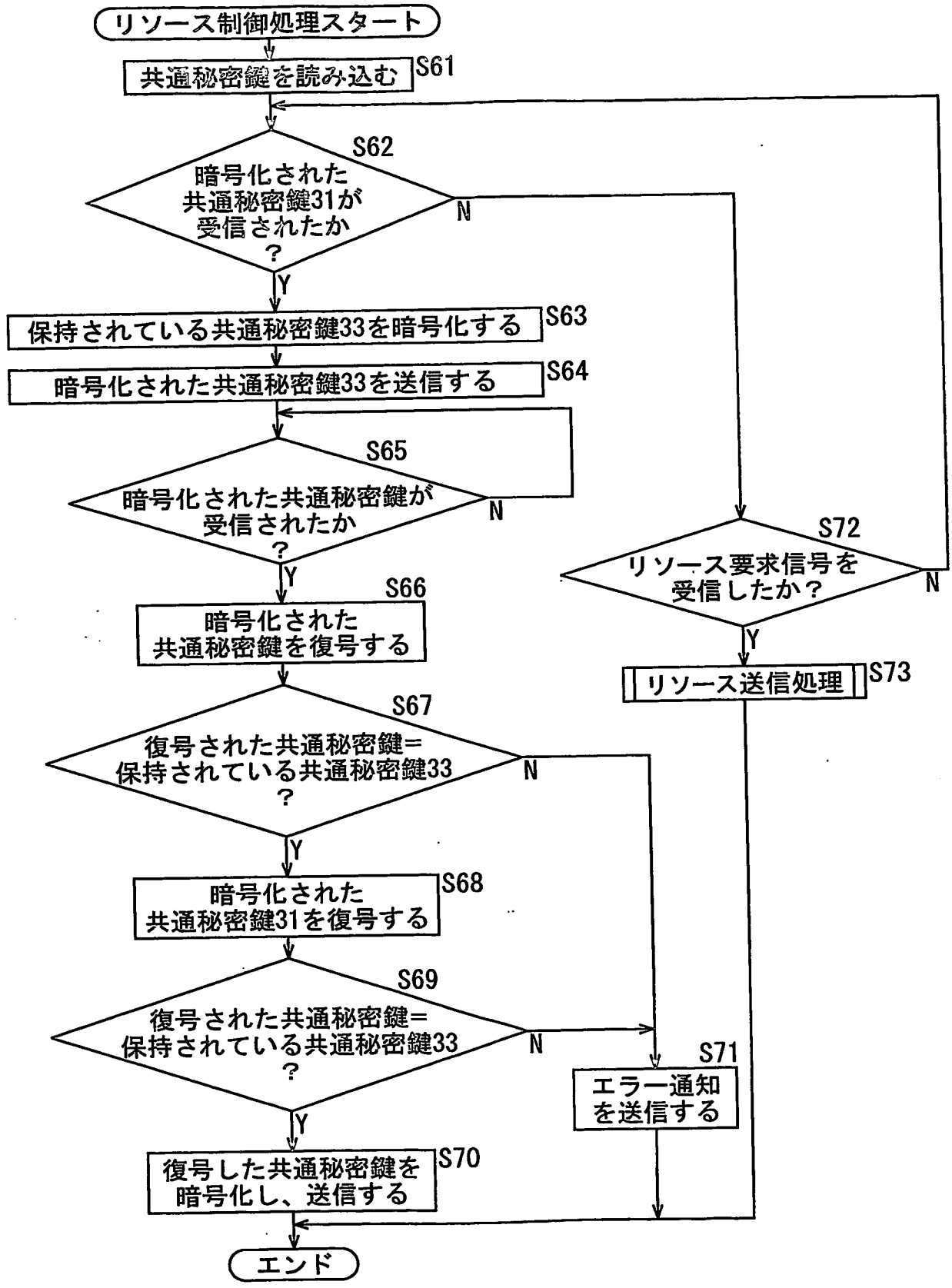

リソース制御処理スタート
共通秘密鍵を読み込む
S61
S62
暗号化された共通秘密鍵31が受信されたか？
N
Y
保持されている共通秘密鍵33を暗号化する
S63
暗号化された共通秘密鍵33を送信する
S64
S65
暗号化された共通秘密鍵が受信されたか？
N
Y
S66
暗号化された共通秘密鍵を復号する
S67
復号された共通秘密鍵＝保持されている共通秘密鍵33？
N
Y
S68
暗号化された共通秘密鍵31を復号する
S69
復号された共通秘密鍵＝保持されている共通秘密鍵33？
N
Y
S70
復号した共通秘密鍵を暗号化し、送信する
エンド
S72
リソース要求信号を受信したか？
N
Y
リソース送信処理
S73
S71
エラー通知を送信する

図９

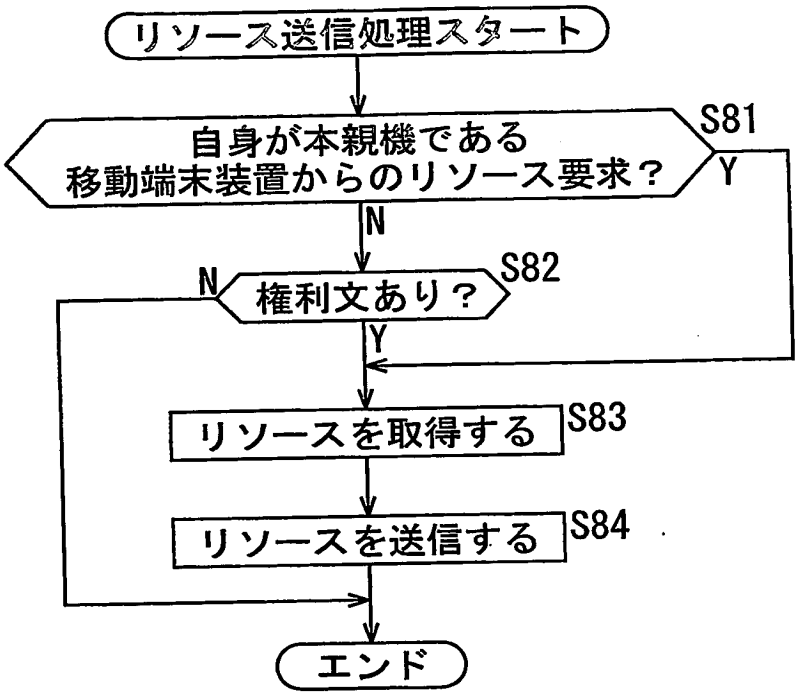

リソース送信処理スタート
自身が本親機である
移動端末装置からのリソース要求？
S81
Y
N
N
権利文あり？
S82
Y
リソースを取得する
S83
リソースを送信する
S84
エンド

図10

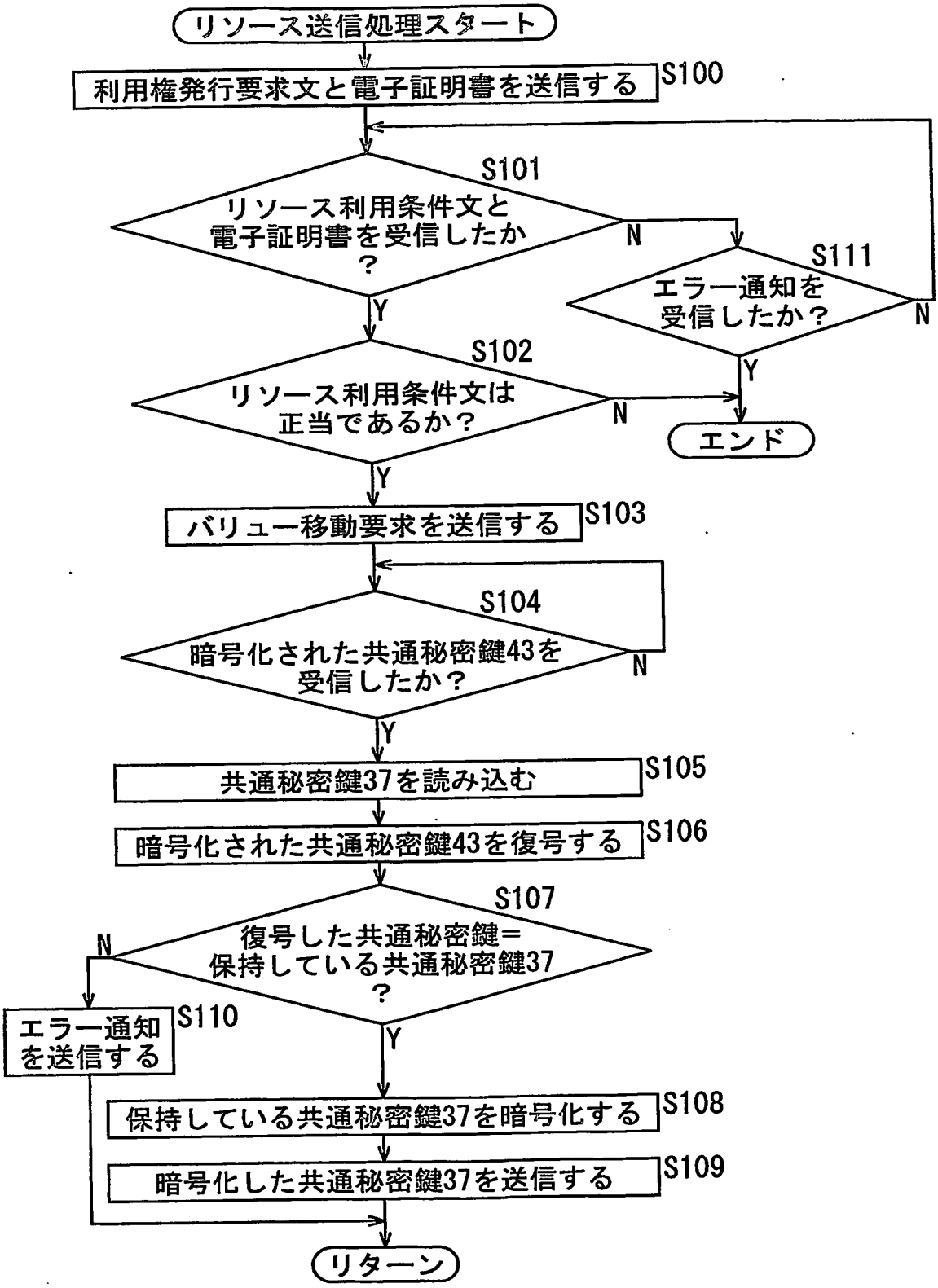

リソース送信処理スタート
利用権発行要求文と電子証明書を送信する
S100
S101
リソース利用条件文と電子証明書を受信したか？
N
Y
S111
エラー通知を受信したか？
N
Y
S102
リソース利用条件文は正当であるか？
N
Y
エンド
バリュー移動要求を送信する
S103
S104
暗号化された共通秘密鍵43を受信したか？
N
Y
共通秘密鍵37を読み込む
S105
暗号化された共通秘密鍵43を復号する
S106
S107
復号した共通秘密鍵＝保持している共通秘密鍵37？
N
Y
エラー通知を送信する
S110
保持している共通秘密鍵37を暗号化する
S108
暗号化した共通秘密鍵37を送信する
S109
リターン

図11

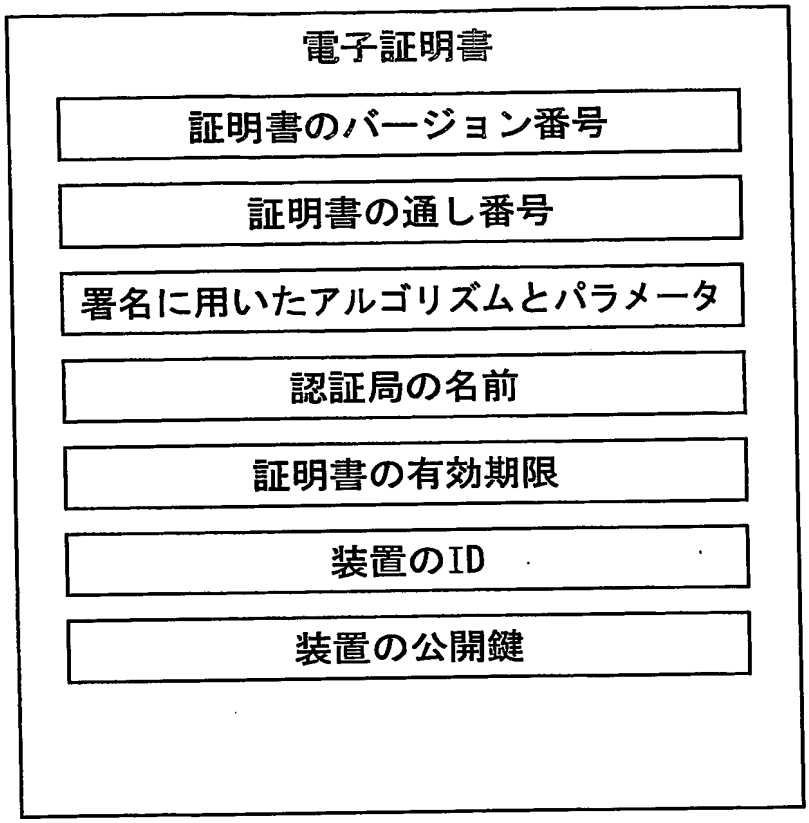

電子証明書
証明書のバージョン番号
証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
装置のID
装置の公開鍵

図12

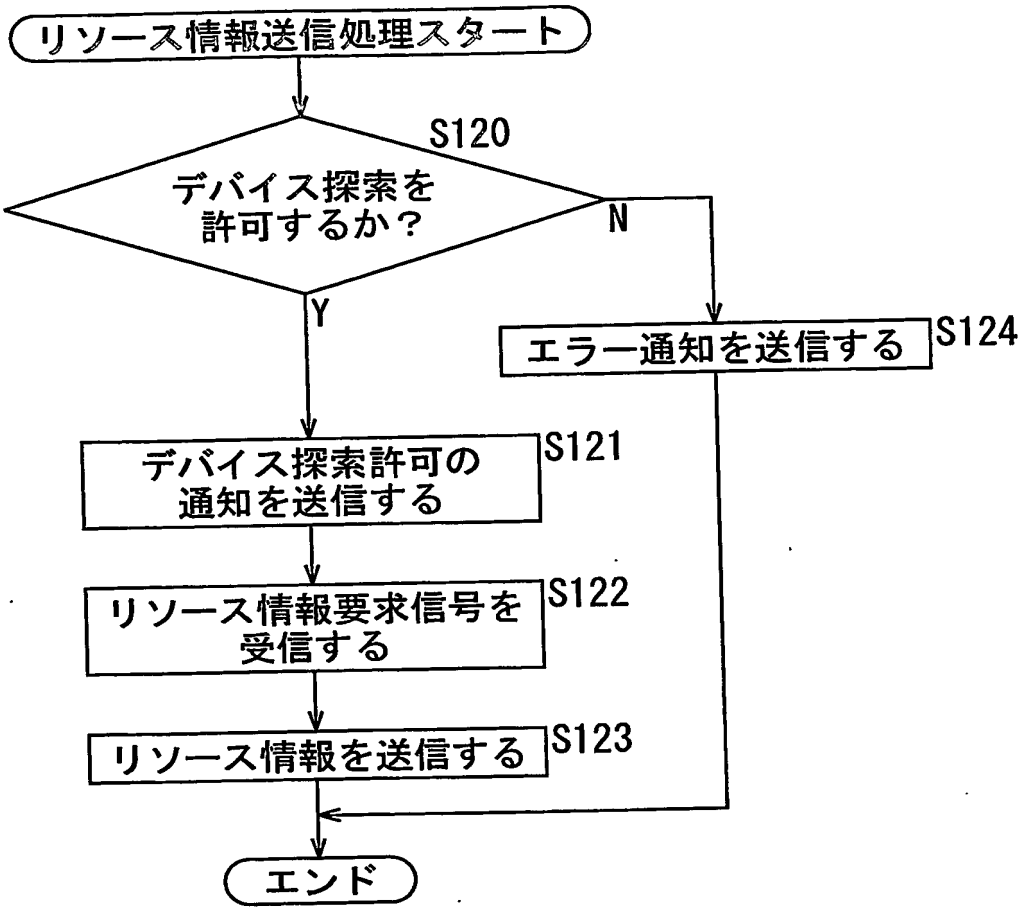

リソース情報送信処理スタート
S120
デバイス探索を
許可するか？
N
Y
エラー通知を送信する
S124
デバイス探索許可の
通知を送信する
S121
リソース情報要求信号を
受信する
S122
リソース情報を送信する
S123
エンド

図13

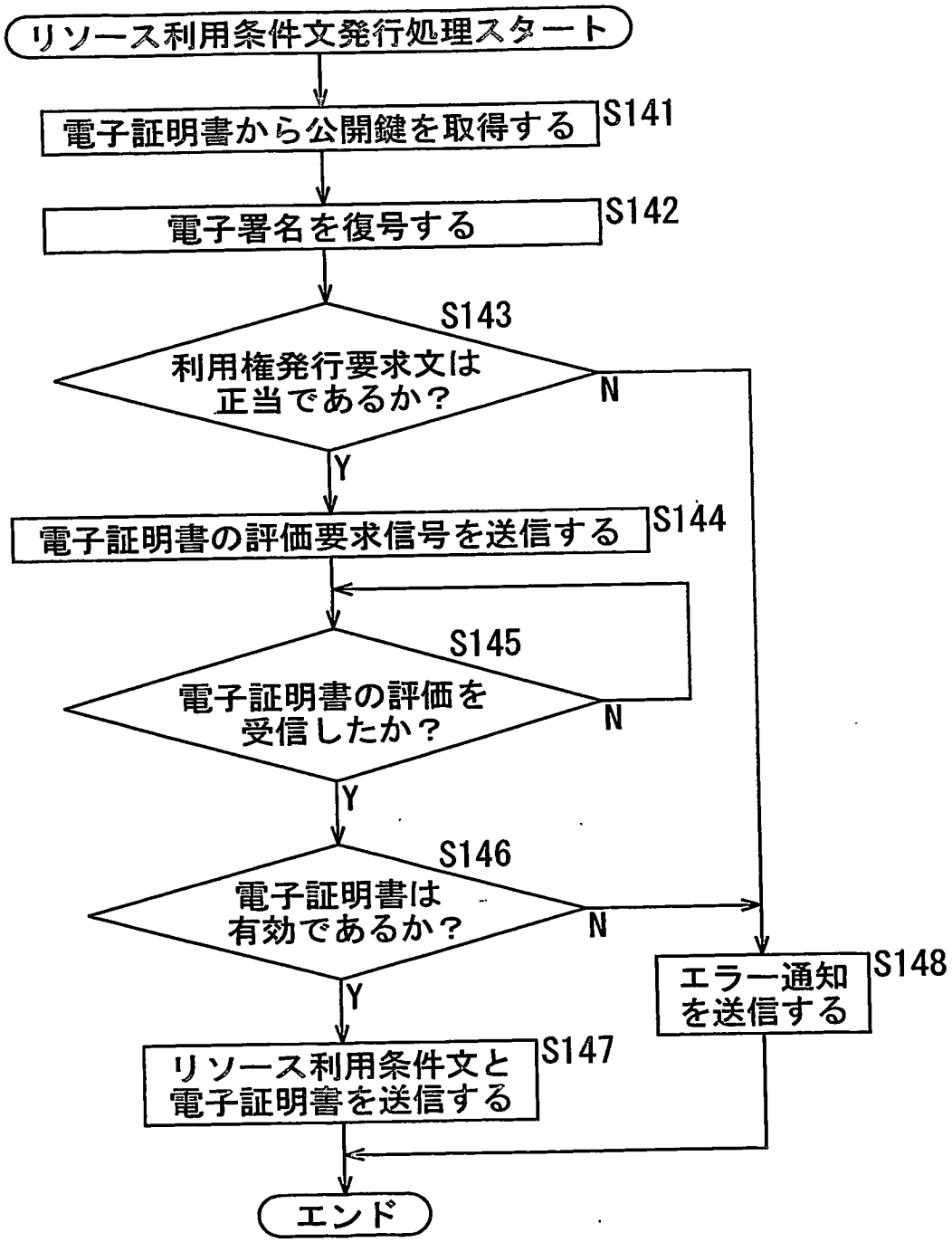

リソース利用条件文発行処理スタート
電子証明書から公開鍵を取得する
S141
電子署名を復号する
S142
S143
利用権発行要求文は正当であるか？
N
Y
電子証明書の評価要求信号を送信する
S144
S145
電子証明書の評価を受信したか？
N
Y
S146
電子証明書は有効であるか？
N
Y
エラー通知を送信する
S148
リソース利用条件文と電子証明書を送信する
S147
エンド

図14

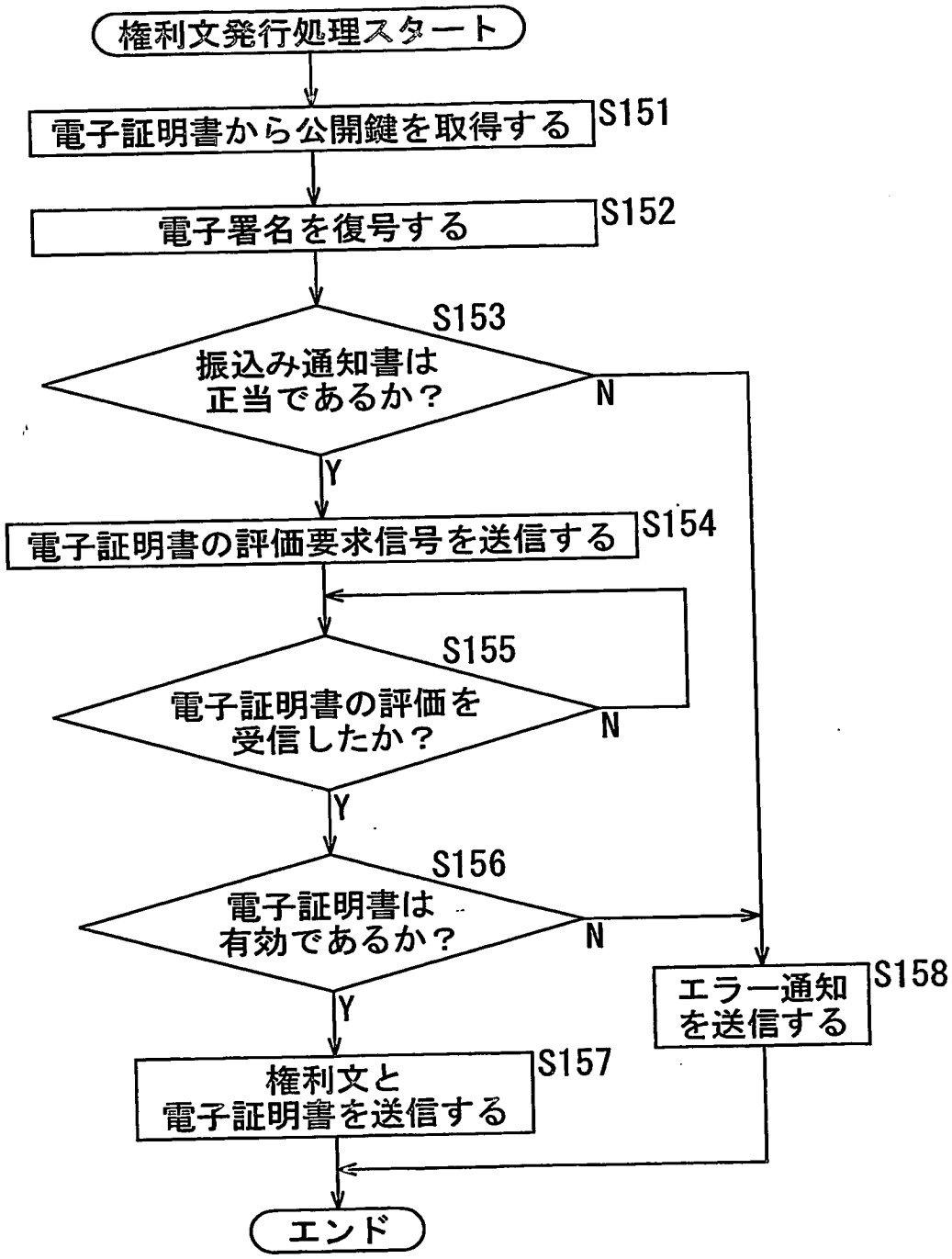

権利文発行処理スタート
電子証明書から公開鍵を取得する
S151
電子署名を復号する
S152
S153
振込み通知書は
正当であるか？
N
Y
電子証明書の評価要求信号を送信する
S154
S155
電子証明書の評価を
受信したか？
N
Y
S156
電子証明書は
有効であるか？
N
Y
エラー通知
を送信する
S158
権利文と
電子証明書を送信する
S157
エンド

図15

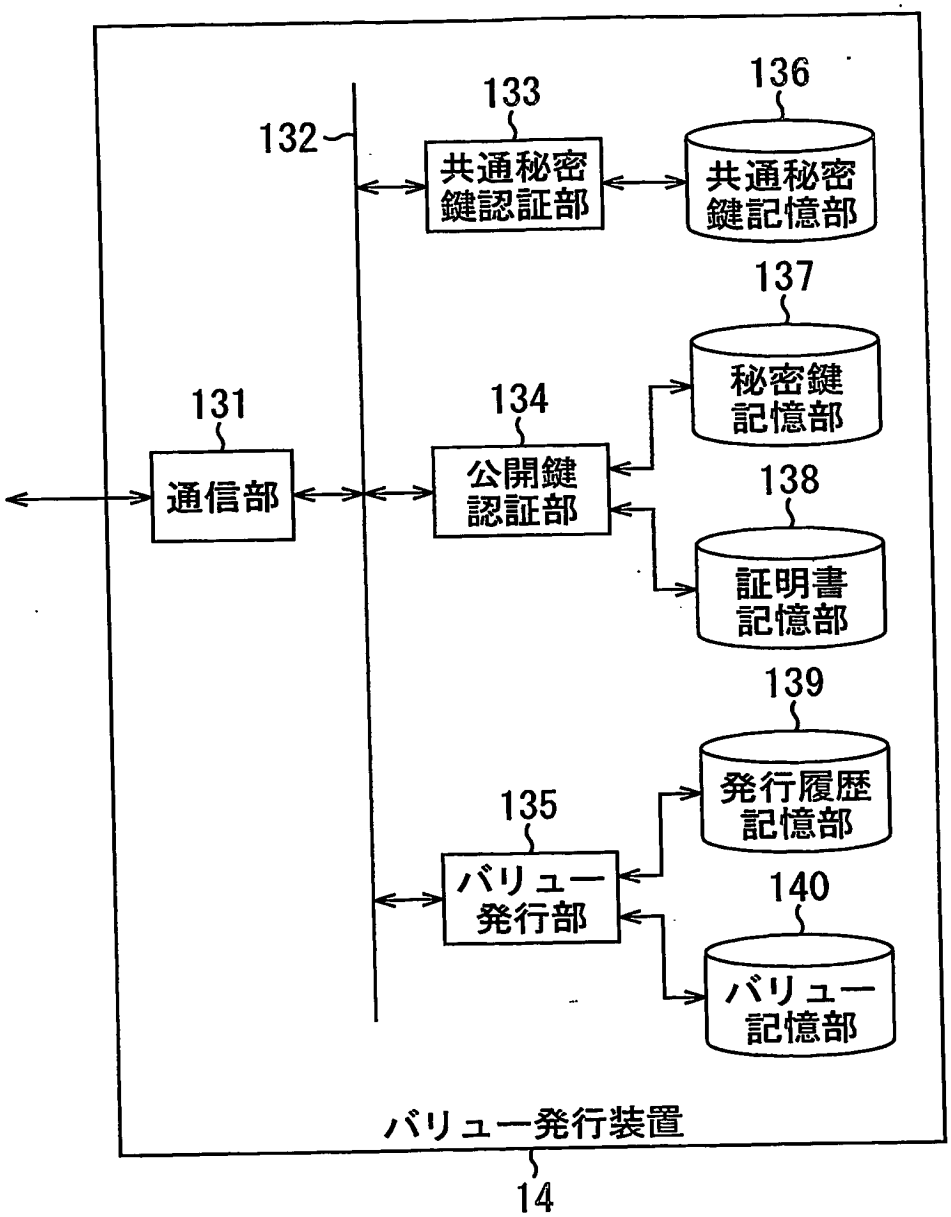

133
136
132
共通秘密鍵認証部
共通秘密鍵記憶部
137
秘密鍵記憶部
131
134
通信部
公開鍵認証部
138
証明書記憶部
139
発行履歴記憶部
135
バリュー発行部
140
バリュー記憶部
バリュー発行装置
14

図16

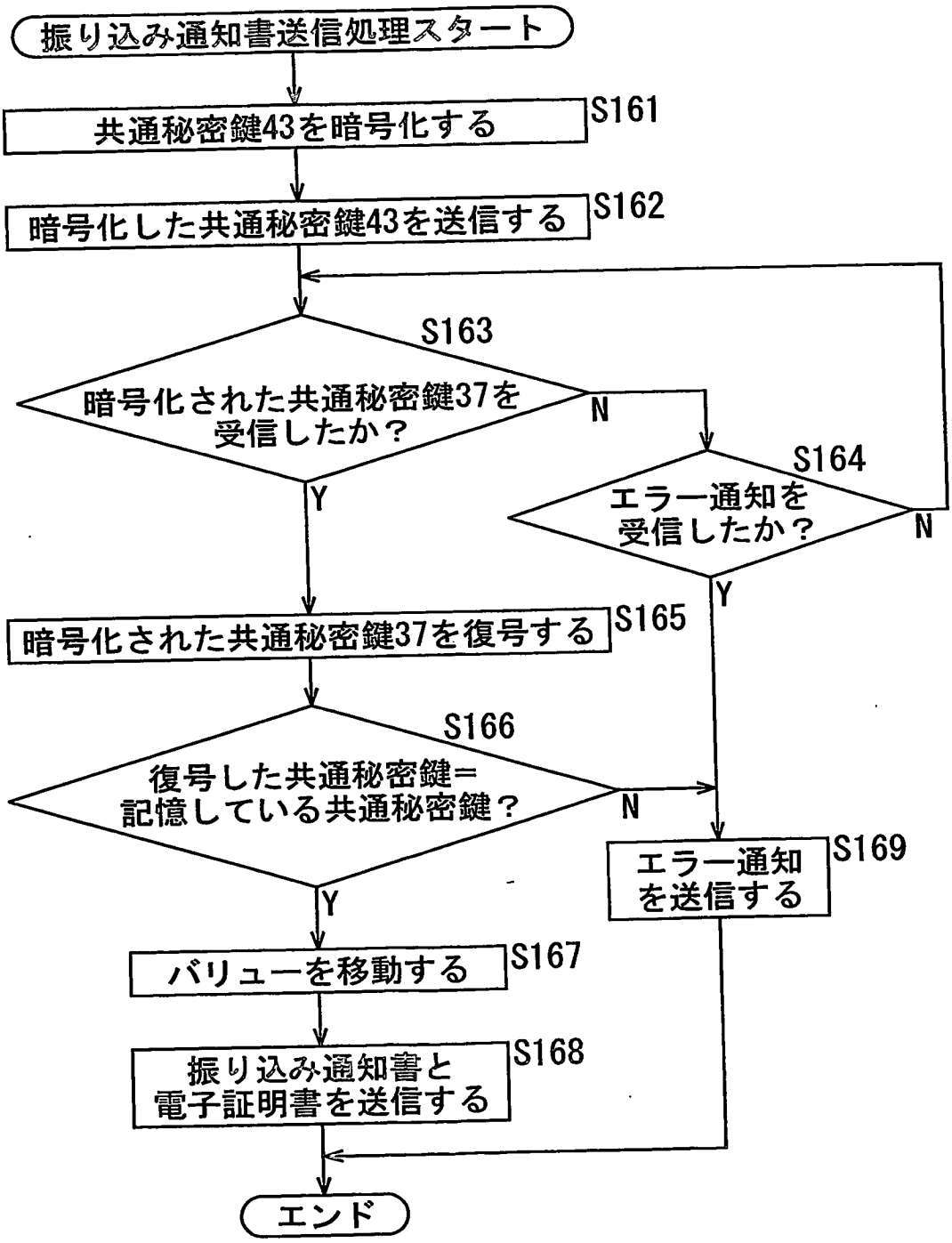

振り込み通知書送信処理スタート
共通秘密鍵43を暗号化する
S161
暗号化した共通秘密鍵43を送信する
S162
S163
暗号化された共通秘密鍵37を受信したか？
N
Y
S164
エラー通知を受信したか？
N
Y
暗号化された共通秘密鍵37を復号する
S165
S166
復号した共通秘密鍵＝記憶している共通秘密鍵？
N
Y
エラー通知を送信する
S169
バリューを移動する
S167
振り込み通知書と電子証明書を送信する
S168
エンド

図17

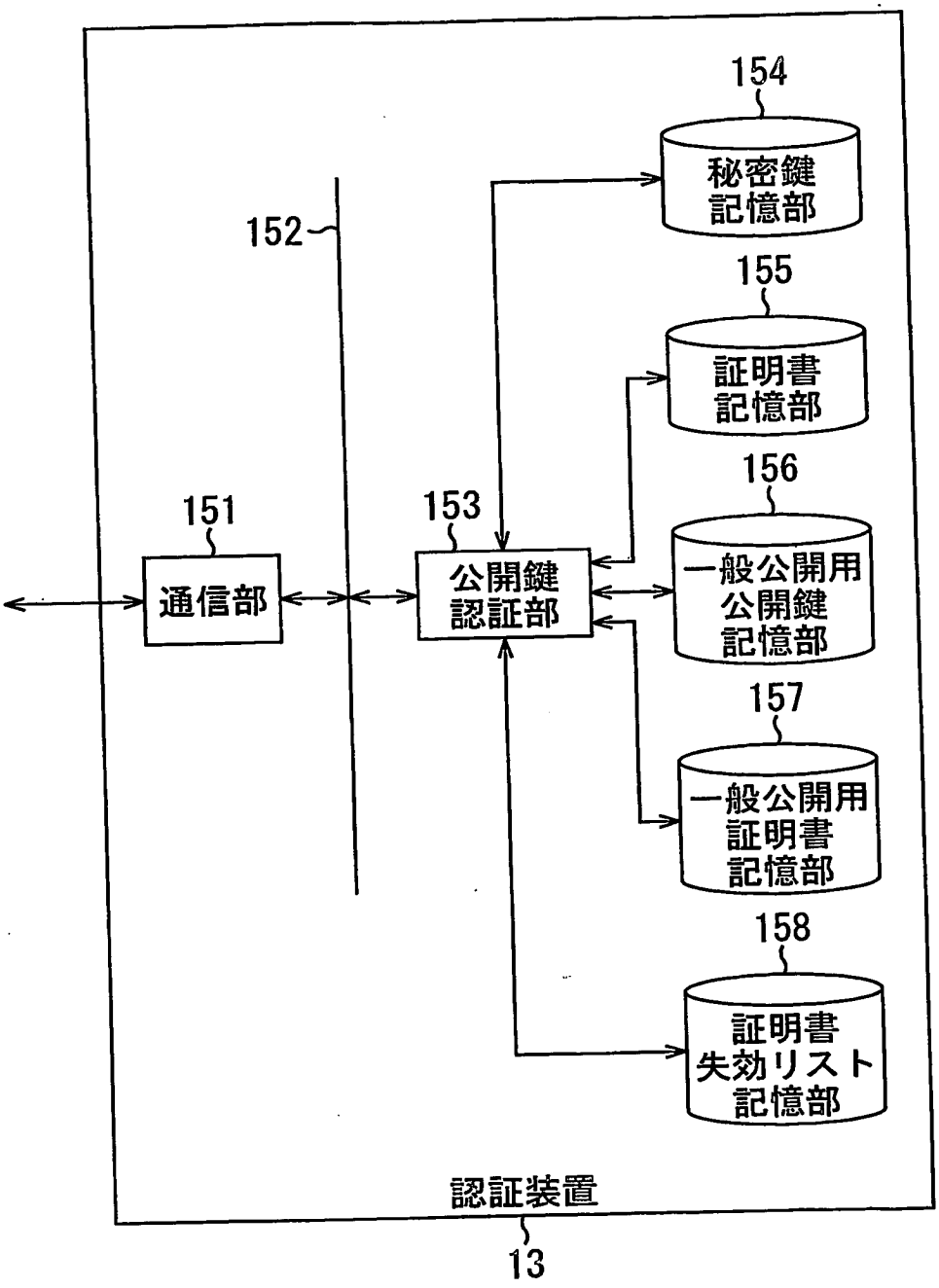

154
秘密鍵
記憶部
152
155
証明書
記憶部
156
151
153
通信部
公開鍵
認証部
一般公開用
公開鍵
記憶部
157
一般公開用
証明書
記憶部
158
証明書
失効リスト
記憶部
認証装置
13

図18

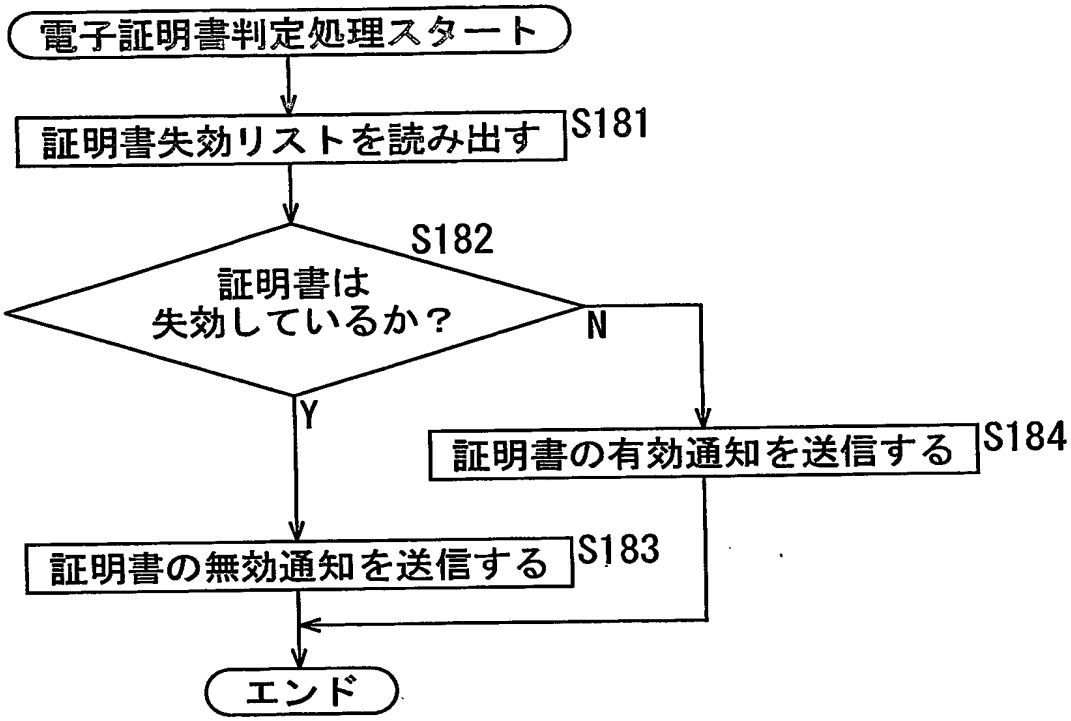

電子証明書判定処理スタート
証明書失効リストを読み出す
S181
S182
証明書は
失効しているか？
N
Y
証明書の有効通知を送信する
S184
証明書の無効通知を送信する
S183
エンド

図19

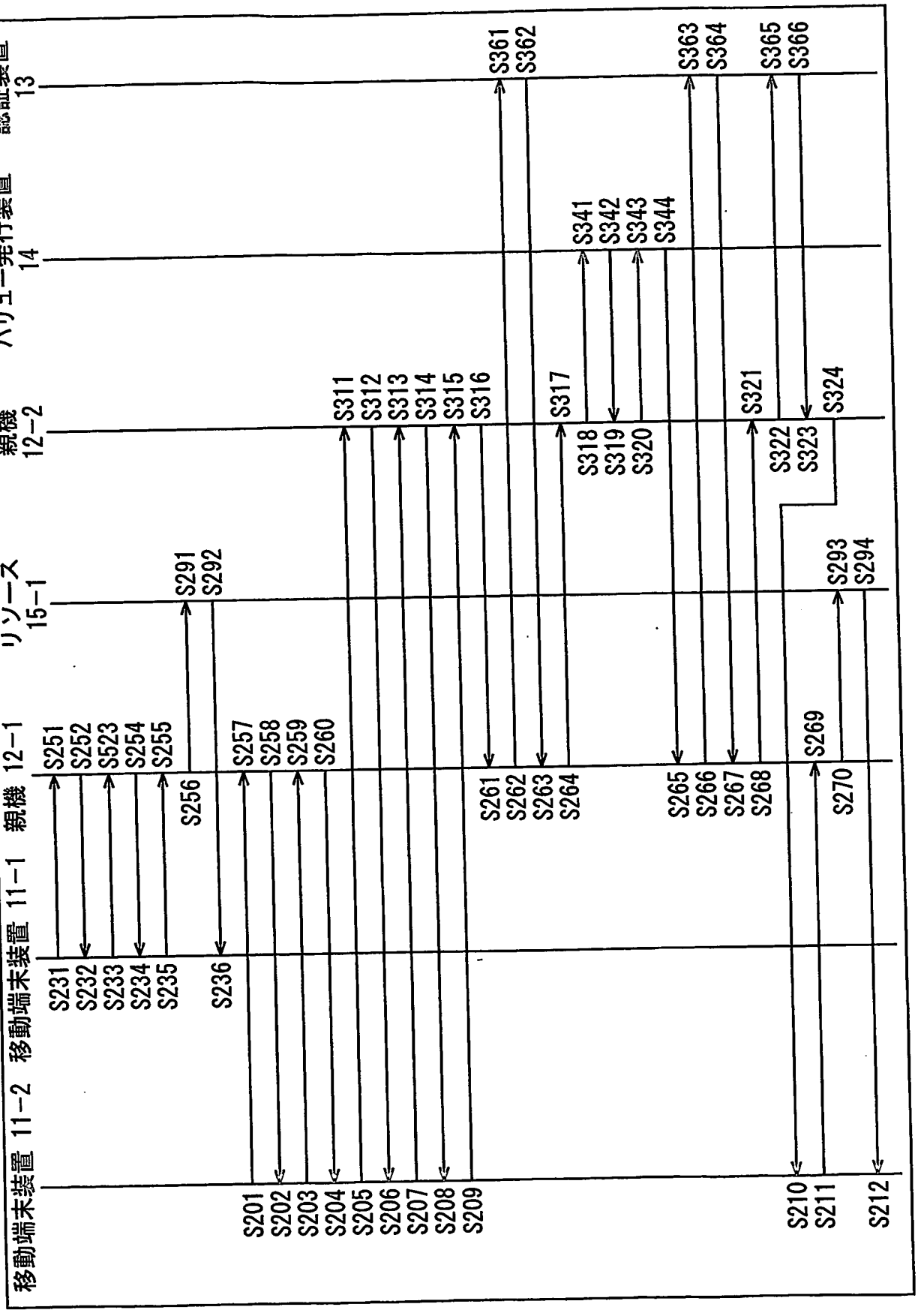

移動端末装置 11-2
移動端末装置 11-1
親機 12-1
親機 12-2
リソース 15-1
パリュー発行装置 14
認証装置 13
S201
S202
S203
S204
S205
S206
S207
S208
S209
S210
S211
S212
S231
S232
S233
S234
S235
S236
S251
S252
S523
S254
S255
S256
S257
S258
S259
S260
S261
S262
S263
S264
S265
S266
S267
S268
S269
S270
S291
S292
S293
S294
S311
S312
S313
S314
S315
S316
S317
S318
S319
S320
S321
S322
S323
S324
S341
S342
S343
S344
S361
S362
S363
S364
S365
S366

図20

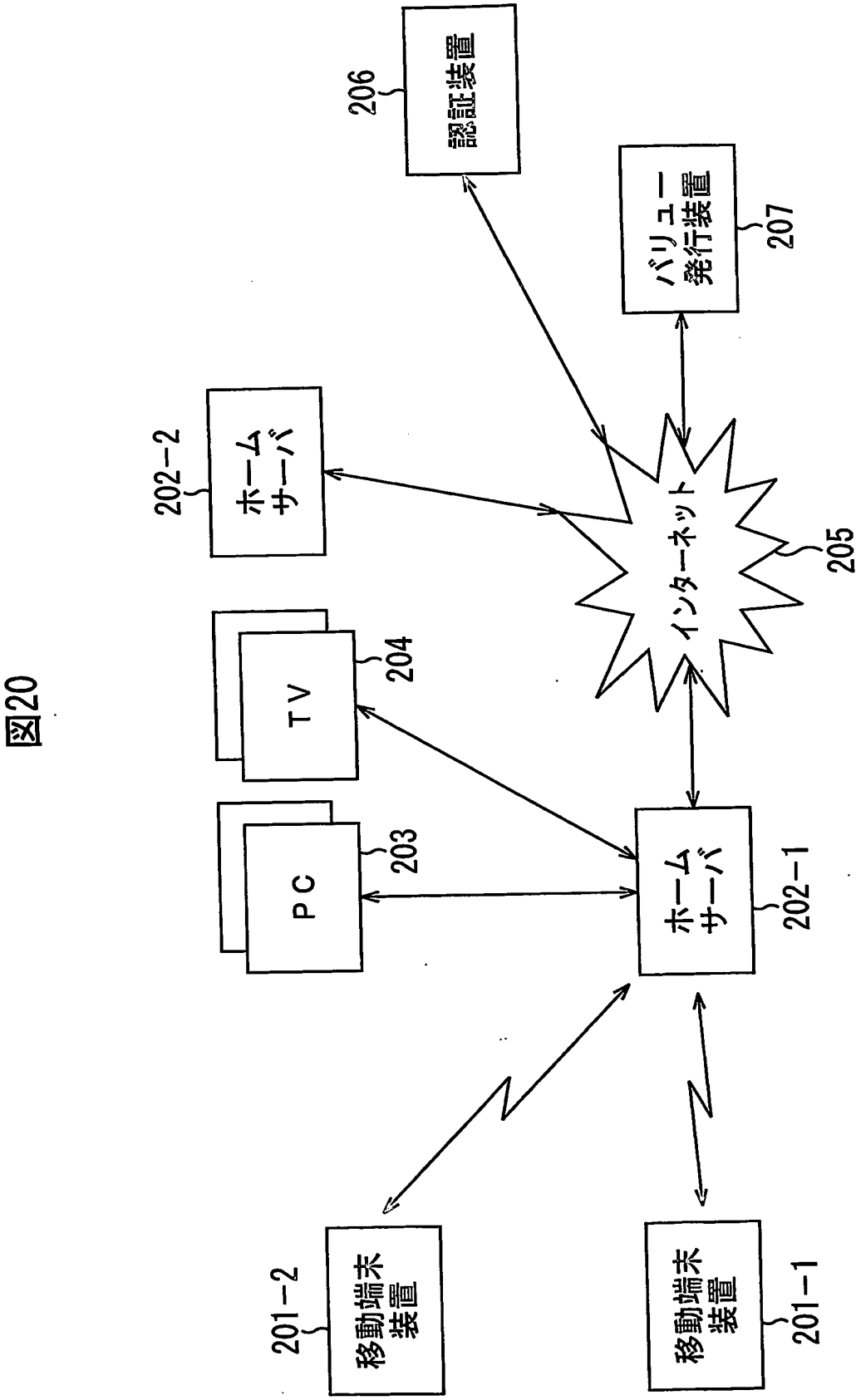
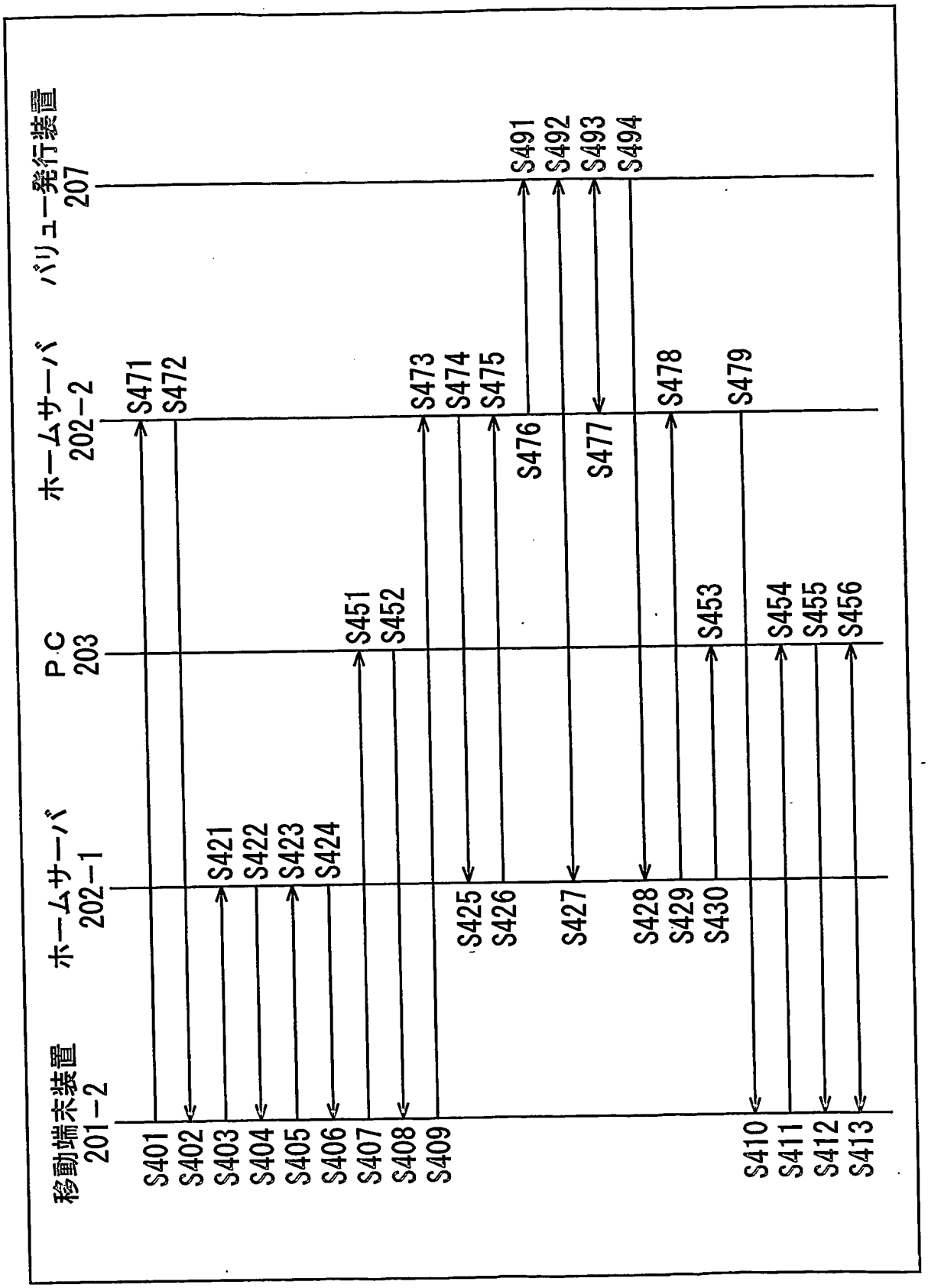

認証装置
206
バリュー
発行装置
207
ホーム
サーバ
202−2
インターネット
205
TV
204
PC
203
ホーム
サーバ
202−1
移動端末
装置
201−2
移動端末
装置
201−1

図21


移動端末装置
201－2
ホームサーバ
202－1
P.C
203
ホームサーバ
202－2
バリュー発行装置
207
S401
S402
S403
S404
S405
S406
S407
S408
S409
S410
S411
S412
S413
S421
S422
S423
S424
S425
S426
S427
S428
S429
S430
S451
S452
S453
S454
S455
S456
S471
S472
S473
S474
S475
S476
S477
S478
S479
S491
S492
S493
S494

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/004338

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-323986 A (Hitachi, Ltd.), 08 November, 2002 (08.11.02), & US 2002/161891 A1	1-28
A	JP 2002-140295 A (Nippon Telegraph And Telephone Corp.), 17 May, 2002 (17.05.02), (Family: none)	1-28
A	JP 2002-73566 A (Sony Corp.), 12 March, 2002 (12.03.02), & US 2002/26427 A1	1-28
A	Tatsuo ITABASHI et al., "Hisesshoku IC card to Keitai Joho Tanmatsu o Riyo shita E-Commerce system no Kaihatsu", Proceedings of Sony Research Forum, 2001, 2002, Vol.11, pages 125 to 130	1-28

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 19 April, 2004 (19.04.04)	Date of mailing of the international search report 11 May, 2004 (11.05.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　PCT／JP2004／004338

A.　発明の属する分野の分類（国際特許分類（IPC））

Int Cl⁷　G06F17／60

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int Cl⁷　G06F17／60, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル（JOIS）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP　2002－323986　A（株式会社日立製作所） 2002.11.08　&　US　2002／161891　A1	1－28
A	JP　2002－140295　A（日本電信電話株式会社） 2002.05.17（ファミリーなし）	1－28
A	JP　2002－73566　A（ソニー株式会社） 2002.03.12　&　US　2002／26427　A1	1－28

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　19.04.2004	国際調査報告の発送日　11.5.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5L　8724 金子　幸一 電話番号　03－3581－1101　内線　3560

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００４３３８

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	板橋達夫他，非接触ＩＣカードと携帯情報端末を利用したｅコマースシステムの開発，Proceedings of Sony Research Forum 2001，２００２，第１１巻，ｐ．１２５－１３０	１－２８